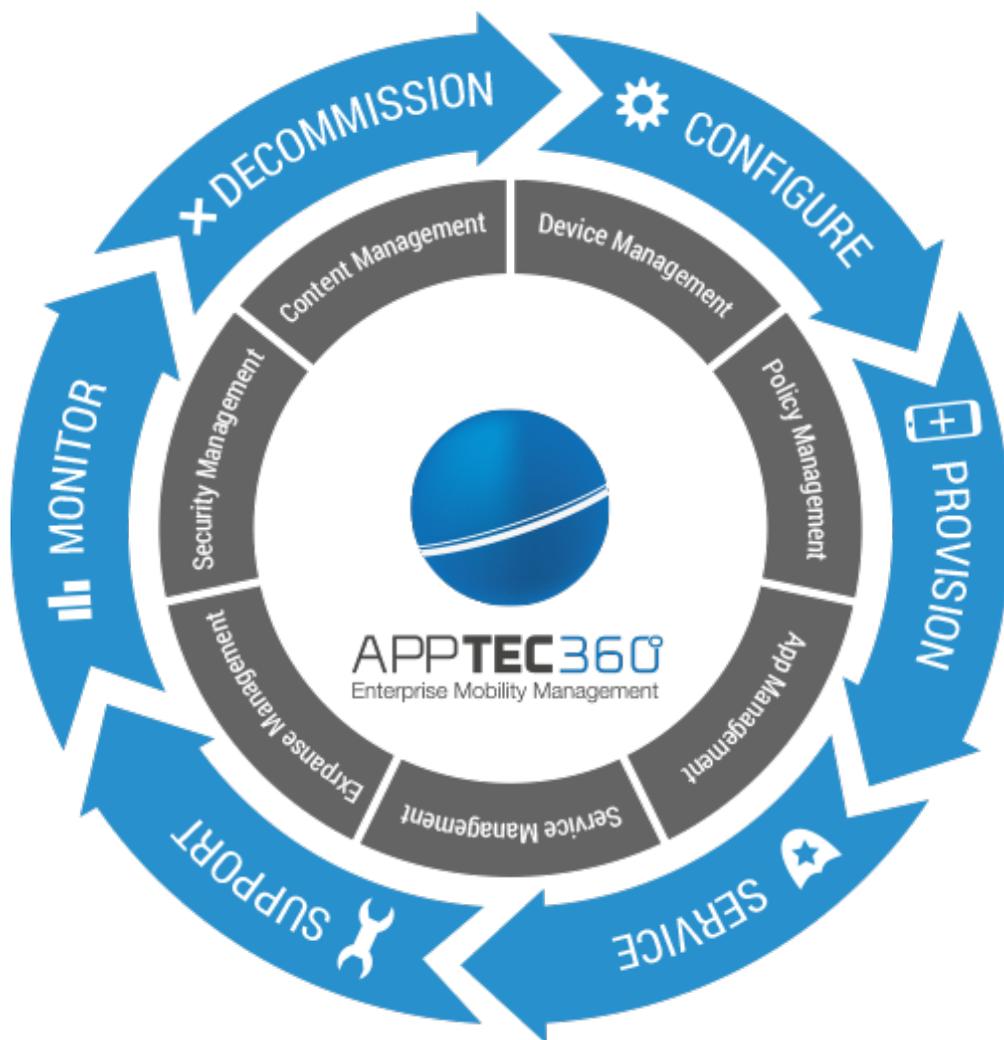




APPT^{EC}360

Enterprise Mobility Management

*AppTec360 Enterprise Mobile Manager & ContentBox
Administrationshandbuch | Version 3.0 (150821.1)*



Inhaltsverzeichnis

I. ALLGEMEINES	9
Einleitende Worte zu AppTec360	9
Unterstützte Geräte und Plattformen	10
Apple Configurator Anleitung	11
II. VORAUSSETZUNGEN / INSTALLATION	12
Voraussetzungen	12
Systemvoraussetzungen	12
Firewallregelungen	12
IP-Adresse und DNS Auflösung	13
SSL-Zertifikat.....	13
Lizenzschlüssel.....	13
Installation am Beispiel VMware	14
III. GENERAL SETTINGS	25
Account Overview	25
Overview	25
Bug Report.....	25
Feature Request	27
Global Configuration	28
eMail Settings.....	28
eMail Templates.....	29
SMS Enrollment.....	30
Privacy	31
GPS Access	31
Apple Configuration	32
APNS Certificate	32
Android Configuration	36
Android Configuration	36
Windows Configuration	37
Windows Configuration	37
Content Box	39
Configuration	39
LDAP Configuration	41

LDAP Overview	41
App Management	43
In-House App DB	43
Android	43
iOS	44
Windows	45
Black-& Whitelisting	46
Android	46
Apple	46
Windows	47
Third Party Apps	48
Android	48
VPP / KNOX	49
VPP Token	49
Knox Key	49
VPP Licenses	50
App Store	50
Region	50
IV. MOBILE MANAGEMENT	51
Oberfläche im Mobile Management	51
Gerätefilter	51
Suchfenster	51
Optionszahnrad	51
Navigationspfeile	51
Administrationskonto-Einstellungen	52
Firmenverwaltung (Root-Verzeichnis) im Mobile Management	53
Create a Subgroup	53
Rename Root Node	54
Mass Enrollment	54
Mass Assignment	55
Gruppenverwaltung im Mobile Management	56
Create a Subgroup	57
Edit selected Group	57
Delete selected Group	58
Create a User	60
Benutzerverwaltung im Mobile Management	61
Add and enroll a Device	62
Profilverwaltung im Mobile Management	64
Create a profile	64
Edit Profile	64
Copy Profile	64
Delete Profile	65
Vererbung von Profilen	66
Geräteverwaltung im Mobile Management	67
Android	67

Edit Device	68
Clear Passcode	68
Lock Device	68
Delete Device.....	68
Wipe Device	70
Enterprise Wipe	70
Send Message	71
Send Enrollment Request	71
iOS	72
Edit Device	73
Clear Passcode	73
Lock Device	73
Delete Device.....	74
Enterprise Wipe	75
Send Message	75
Send Enrollment Request	76
Remove MDM	76
Windows.....	78
Edit Device	79
Lock Device	79
Delete Device.....	79
Wipe Device	80
Enterprise Wipe	80
Content Management	82
File Explorer	85
Audit Trail.....	85
Trash.....	86
External Storage	86
Konfiguration iOS	88
General	88
General Information.....	88
Settings	89
Config Revision	89
Device Log	89
Asset Management (nur auf Device Ebene).....	90
Asset Management (nur auf Device Ebene).....	90
Security Management.....	91
Anti Theft (nur auf Device Ebene).....	91
GPS Information (nur auf Device Ebene)	91
Wipe & Lock (nur auf Device Ebene)	91
Message (nur auf Device Ebene)	92
Security Configuration.....	93
Passcode	93
Encryption.....	94
End of Life (nur auf Device Ebene).....	95
Wipe (nur auf Device Ebene)	95
Restriction Settings.....	96
Device Functionality	96
Applications	98

iCloud	98
Security and Privacy	98
BYOD Container	99
Activation	99
SecurePIM Password	99
SecurePIM Security	100
SecurePIM Browser	101
Exchange	102
Connection Management	103
Wifi	103
VPN	105
APN	106
Cellular	106
HTTP Proxy	107
AirPrint	107
AirPlay	107
PIM Management	108
Exchange Active Sync	108
eMail	108
CalDav	109
CardDav	110
Subscribed Calendars	110
LDAP	110
Web Management	111
Webclips	111
Web Content Filter	111
App Management	112
Enterprise App Manager	112
Installed Apps (nur auf Device Ebene)	112
Mandatory Apps	113
Web Apps	114
Blacklisted Apps	114
App-VPN	114
App Settings	115
Enterprise App Store	117
iTunes Apps	117
In-House	119
Kiosk Mode	122
Content Management	123
ContentBox	123
Konfiguration Android	124
General	124
Device Overview (nur auf Device Ebene)	124
Config Revision	125
Device Log	125
Device Settings	126
Client Configuration	126

- Asset Management (nur auf Device Ebene).....127**
 - Asset Management (nur auf Device Ebene)..... 127

- Security Management.....129**
 - Anti Theft (nur auf Device Ebene)..... 129
 - GPS Information (nur auf Device Ebene) 129
 - Wipe & Lock (nur auf Device Ebene) 129
 - Message (nur auf Device Ebene) 130
 - Security Configuration..... 131
 - Passcode 131
 - Encryption..... 132
 - AntiVirus..... 133
 - End of Life (nur auf Device Ebene)..... 134
 - Wipe (nur auf Device Ebene) 134
 - Restriction Settings..... 136
 - Restrictions..... 136
 - Allow Screen Capture 137
 - Erlauben von Screenshots 137
 - Allow Clipboard 137
 - Erlauben der Zwischenablage 137
 - BYOD Container 138
 - Activation 138
 - Knox Passcode 138
 - Knox Security 139
 - Knox eMail..... 140
 - Knox Apps 141

- Connection Management.....142**
 - Wifi..... 142
 - VPN 144
 - Restrictions..... 145
 - APN 146
 - Bluetooth..... 147

- PIM Management.....148**
 - Exchange..... 148
 - eMail..... 149
 - Touchdown Exchange 150

- App Management151**
 - Enterprise App Manager..... 151
 - Installed Apps (nur auf Device Ebene)..... 151
 - System Apps (nur auf Device Ebene) 154
 - Mandatory Apps..... 155
 - Sys App Restrictions..... 157
 - Samsung Apps 158
 - Huawei Apps..... 158
 - Enterprise App Store 159
 - Playstore..... 159
 - In-House 162
 - Kiosk Mode..... 165
 - Content Management..... 167
 - ContentBox..... 167

- Konfiguration Windows Phone168**
- General168**
 - Device Overview (nur auf Device Ebene)..... 168
 - Config Revision (nur auf Device Ebene)..... 169
 - Device Log (nur auf Device Ebene)..... 169
- Asset Management (nur auf Geräte Ebene).....170**
 - Asset Management (nur auf Geräte Ebene) 170
- Security Management.....172**
 - Security Configuration..... 172
 - Passcode 172
 - End of Life (nur auf Geräte Ebene)..... 173
 - Wipe (nur auf Geräte Ebene) 173
 - Restriction Settings..... 174
 - Device Functionality 174
- Connection Management.....176**
 - Wifi..... 176
 - Wifi Restrictions 178
 - VPN 179
 - VPN Restrictions 180
 - Bluetooth..... 180
 - NFC 180
- PIM Management.....181**
 - Exchange Active Sync..... 181
 - eMail..... 182
- App Management183**
 - Enterprise App Manager 183
 - Mandatory Apps..... 183
 - Whitelisted / Blacklisted Apps..... 183
 - Enterprise App Store 186
 - Windowsstore 186
 - In-House 188
 - Kiosk Mode 190
 - Kiosk Mode..... 190
- V. DASHBOARD & REPORTING 191**
- Dashboard191**
- Extended Reporting.....192**
 - Compliance Reports..... 193
 - Rooted Devices 193
 - Roaming Devices 193
 - Roaming Enabled Devices..... 194
 - Supervised Devices 194
 - Device Reports..... 194
 - Devices by Ownership..... 194
 - All Devices..... 195
 - Device Carriers 196

SAFE Devices.....	196
App Reports.....	197
Installed Apps	197
Most Installed Apps.....	198
Mandatory Apps.....	199
VI. MANDANTEN MANAGEMENT	200
Oberfläche	200
List all clients	200
APNS expiry dates	201
Account Information	202
Einspielen einer weiteren AppTec-Lizenz	203
Import eines Client-Backups	204
KONTAKT	205
DISCLAIMER	205

I. Allgemeines

Einleitende Worte zu AppTec360

Die Enterprise-Mobile-Management-Lösung von AppTec bietet mit ihrer sehr intuitiv bedienbaren Managementkonsole die Möglichkeit, sämtliche mobilen Devices zentral zu verwalten und zu konfigurieren. Der EMM-Server kann hierbei entweder bei Ihnen in Ihrer eigenen Umgebung laufen oder Sie nutzen unsere cloudbasierte Lösung.

Auch wenn es um das Thema der zentralen Installation von unternehmenseigenen Applikationen auf Smartphones geht, sind Sie bei uns genau richtig. Mit dem Enterprise Mobile Manager können Sie innerhalb von wenigen Sekunden, Unternehmensapplikationen und Dokumente auf die Geräte verteilen oder unerwünschte Applikationen durch White- oder Blacklisting blockieren.

Die Nutzung privater Geräte im Unternehmen stellt neue Herausforderungen an die Absicherung von Smartphones und Tablets dar. IT-Administratoren müssen eine Vielzahl unterschiedlicher Geräte schützen, da Mitarbeiter verstärkt ihre Smartphones im Unternehmen nutzen wollen. Wir helfen Ihnen dabei, alle Geräte und die darauf gespeicherten sensiblen Daten ganz einfach zu sichern und aus einer intuitiven Konsole zu verwalten.

Unterstützte Geräte und Plattformen

AppTec360 bietet Unterstützung für iOS, Android und Windows Phone Geräte. Beachten Sie dabei, dass der Funktionsumfang der genannten Plattformen voneinander differenzieren kann

Minimale unterstützte Softwareversionen:

iOS Geräte ab iOS Version 3.0
 Android Geräte ab Version 2.3
 Windows Phones ab Version 8

Bis einschließlich Android Version 4.1.x muss auf den Samsung Geräten der „AppTec MDM Agent for Samsung“ installiert werden, um das Gerät erfolgreich am Server einbinden zu können.

Erläuterung des „Supervised-Modus“ von Apple Geräten

Der Supervised Modus stellt eine erweiterte Schnittstelle für iOS Geräte von Apple dar.

Für ein entsprechend konfiguriertes Gerät können zusätzliche Einschränkungen im Bezug auf die Funktionalität des Endgerätes angewendet werden. Diese sind ebenfalls in diesem Administrationshandbuch enthalten und werden diesbezüglich mit einem Banner gekennzeichnet.

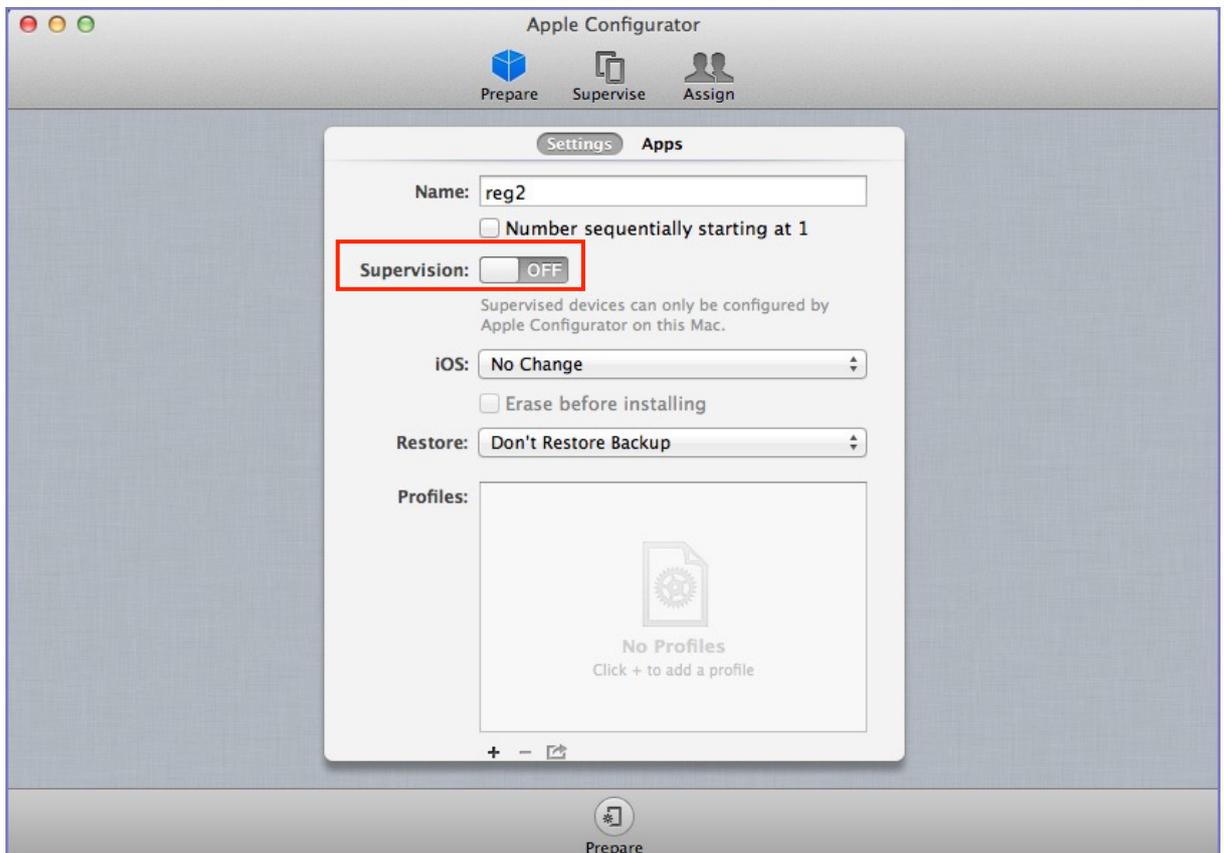
Verfügbar im Supervised-Modus

Der „Supervised-Modus“ kann über das Programm "Apple Configurator" aktiviert werden. Der Apple Configurator kann als Konfigurations-Tool die Grundeinstellung neuer iOS Geräte setzen (über die USB Schnittstelle)

Das Tool kann sowohl Konfigurationsprofile als auch Apps installieren. Es ist kostenlos, setzt aber einen Mac-Rechner voraus.

Apple Configurator Anleitung

1. Öffnen Sie den Apple Configurator



2. Benennen Sie das Profil unter „Name“.
3. Aktivieren Sie den Schalter „Supervision“.
4. Klicken Sie nun auf „Prepare“ – das Gerät wird nun auf die Werkseinstellungen zurückgesetzt und der Supervised-Modus wird nun aktiviert.

II. Voraussetzungen / Installation

Voraussetzungen

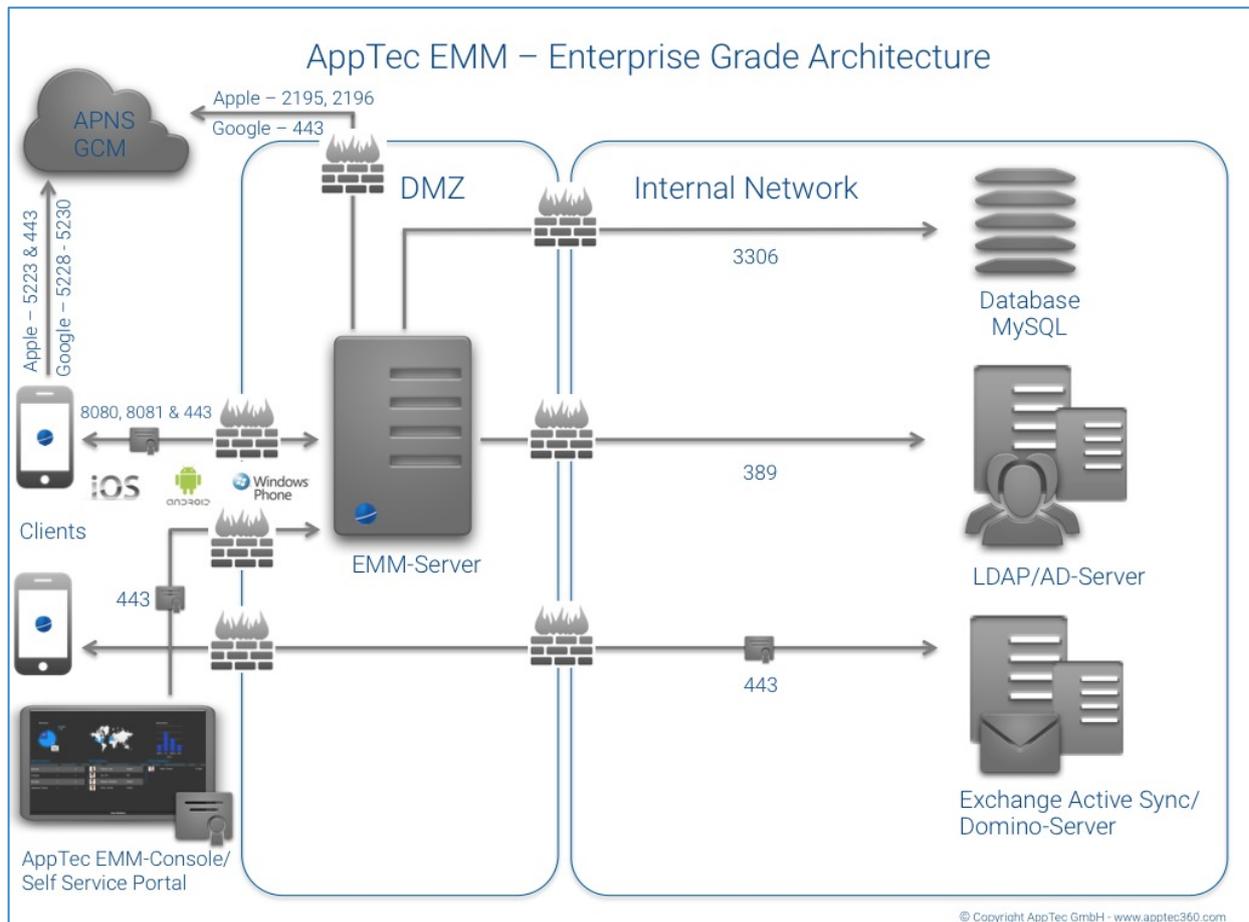
Systemvoraussetzungen

Die virtuelle Appliance wird im Open-Virtual-Format (OVF) bereitgestellt. Diese kann in folgende Systeme importiert werden:

- VMWare
- MS Hyper V
- Virtual Box
- Citrix Xen Server

Zudem werden 2GB RAM/Arbeitsspeicher und 5GB freier Festplattenspeicher benötigt. Die Appliance basiert auf Ubuntu 64bit

Firewallregelungen



Der AppTec Server muss über folgende Ports extern erreichbar sein:

Default Apache http Port	80
Default Apache https Port	443
Default Device Server Port	8080
Default SCEP Server Port	8081

Diese Ports können Sie auf der virtuellen Maschine ändern.

Beachten Sie: Sofern Sie Windows Phones nutzen möchten, darf der „Default Apache https Port“ nicht geändert werden!

Die nachfolgenden Ports müssen von intern nach außen geöffnet sein, damit der AppTec Server mit den entsprechenden Nachrichtendiensten sprechen darf:

Google Ports (Android)	5228, 5229, 5230, 443
Apple Ports (iOS)	2195, 2196, 5223, 443

IP-Adresse und DNS Auflösung

Der AppTec Server muss unter einer öffentlichen IP-Adresse erreichbar sein, zudem benötigen Sie einen entsprechend aufgeschalteten Hostnamen bzw. DNS-Eintrag.

SSL-Zertifikat

Sie müssen ein SSL-Zertifikat, entsprechend ausgestellt zum DNS Eintrag, beantragen oder während dem Installationsprozess erstellen (Nur öffentlich vertrauenswürdige Zertifikate werden unterstützt). Es wird zudem das Intermediate-Zertifikat der CA und der Private Key (nicht passwortgeschützt) benötigt.

Bitte beachten Sie, dass Wildcard-Zertifikate nicht unterstützt werden.

SMTP-Relay

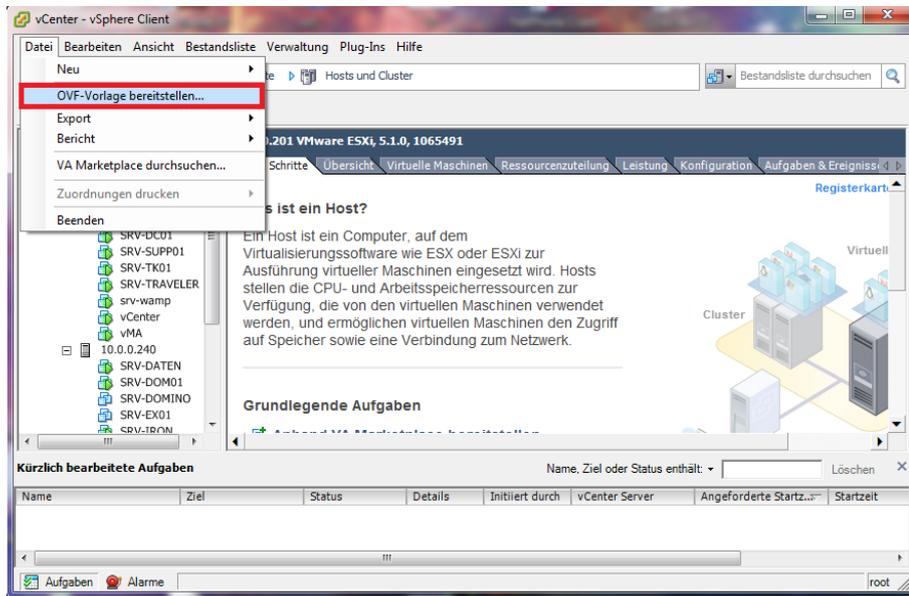
Ein Emailserver bzw. ein Email-Relay wird benötigt, damit der AppTec360 Server Emails an die entsprechenden Benutzer senden kann.

Lizenzschlüssel

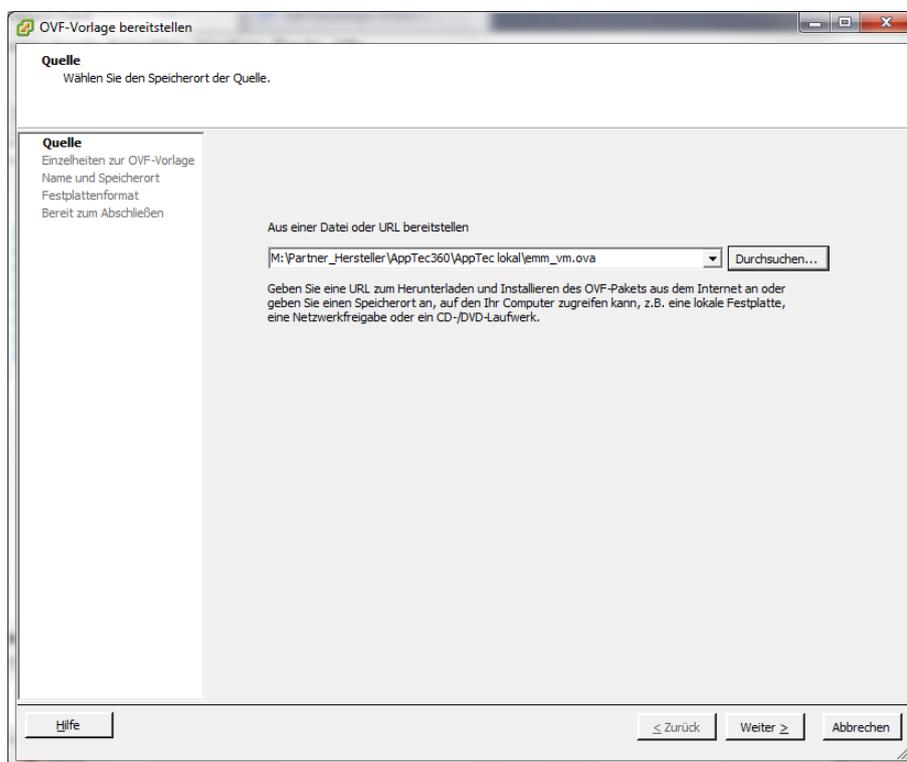
Um den Server erfolgreich aktivieren und installieren zu können benötigen Sie eine gültige Lizenzdatei. Diese können Sie von AppTec360 selbst bzw. von Ihrem entsprechendem Reseller erhalten.

Installation am Beispiel VMware

- „Datei“ > „OVF-Vorlage bereitstellen...“

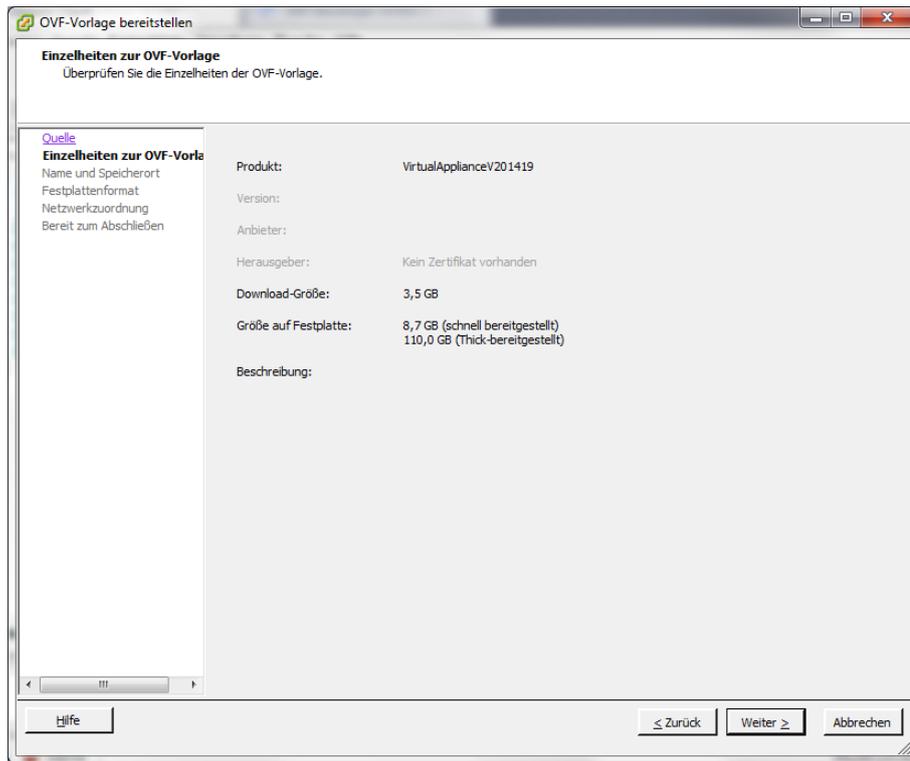


- Im Nachhinein die bereitgestellte OVA-Image auswählen und mit „weiter“

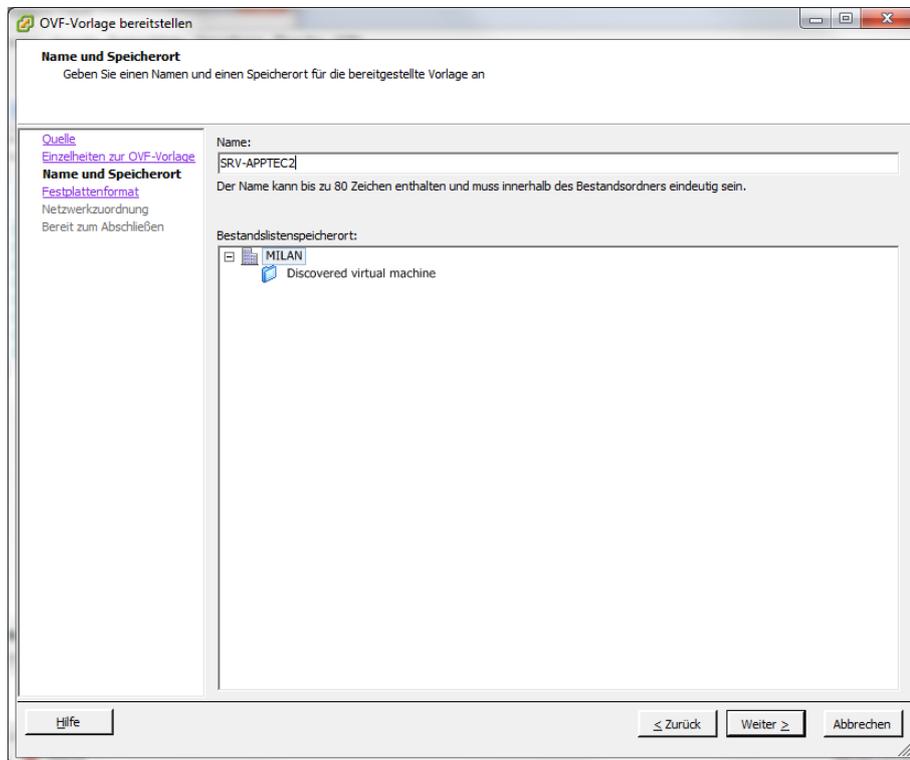


bestätigen.

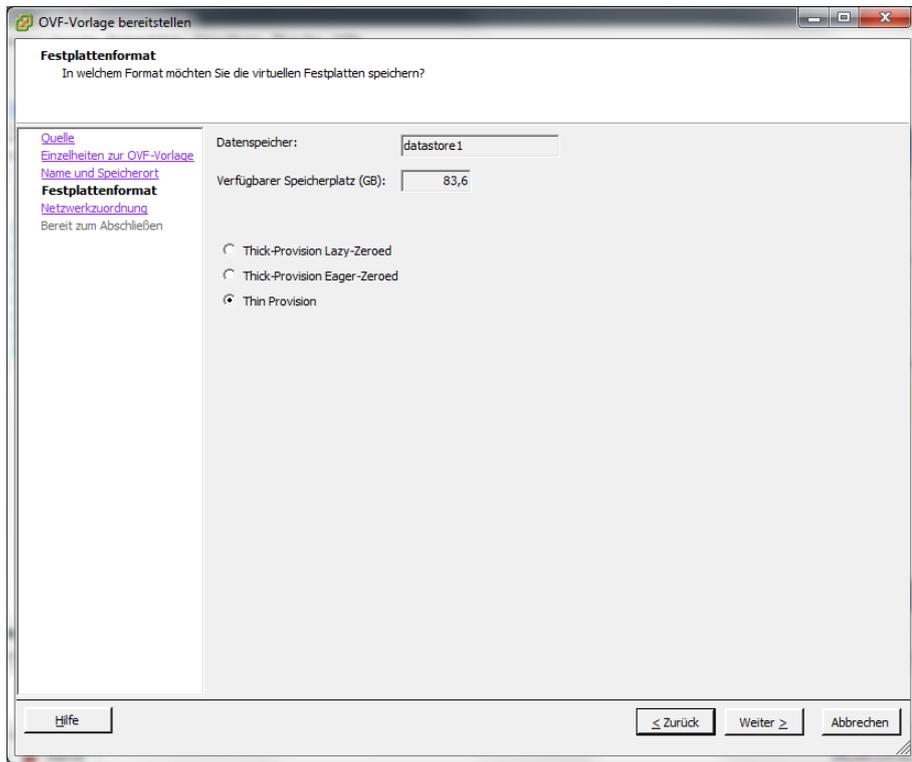
- Einzelheiten zu OVF-Vorlage mit „Weiter“ bestätigen.



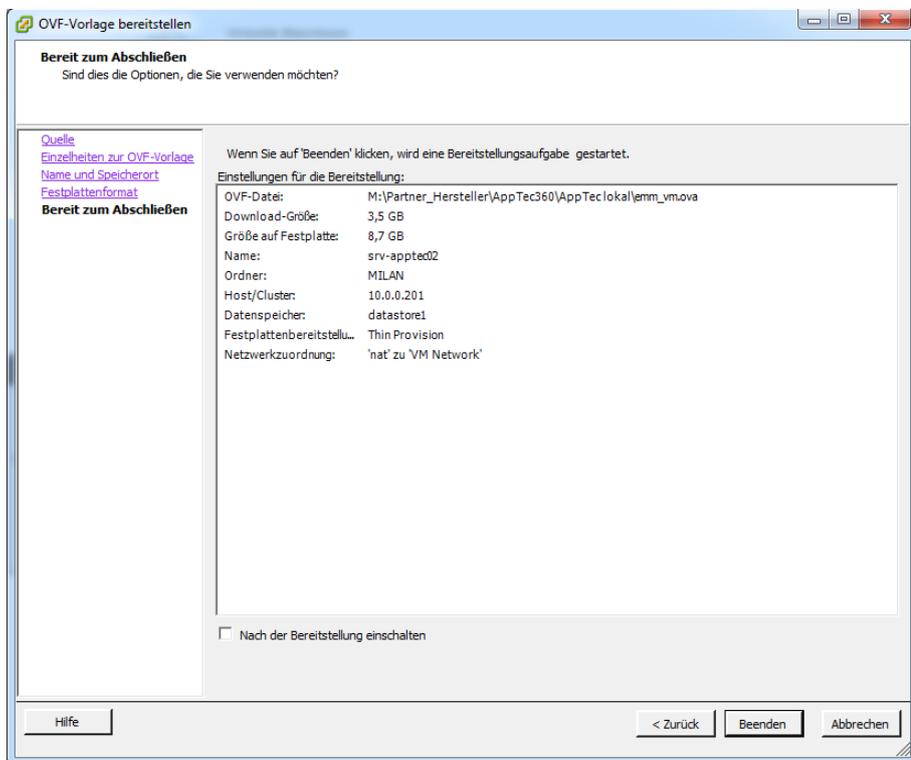
- Hier können Sie die VM nach Ihren Wünschen benennen.



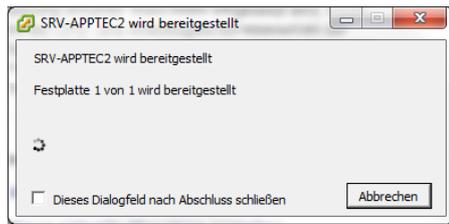
- Festplattenformat der VM mit "weiter" bestätigen.



- Letzte Ansicht der Konfiguration mithilfe von „Beenden“ abschließen.

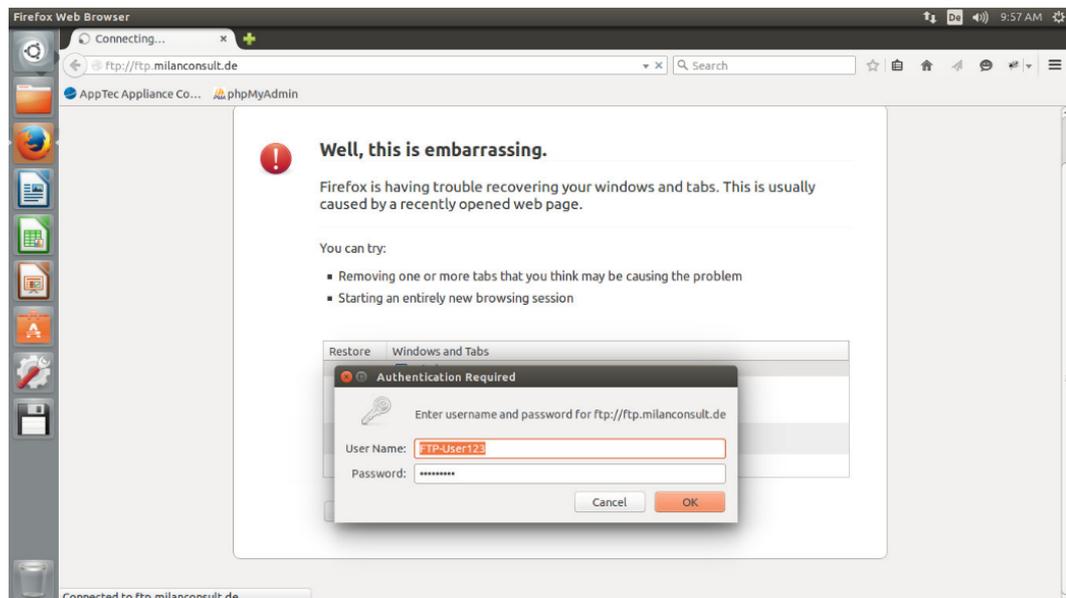


- Bitte warten Sie bis die VM erfolgreich installiert wurde.



Bitte beachten Sie, dass Upgrades des Ubuntu-Betriebssystems auf eine höhere Version einen nicht mehr funktionierenden AppTec-Server zur Folge haben kann. Wir empfehlen an dieser Stelle, KEINE Upgrades auf eine neuere Betriebssystemversion durchzuführen! Jedoch sollten Sicherheitsupdates eingespielt werden!

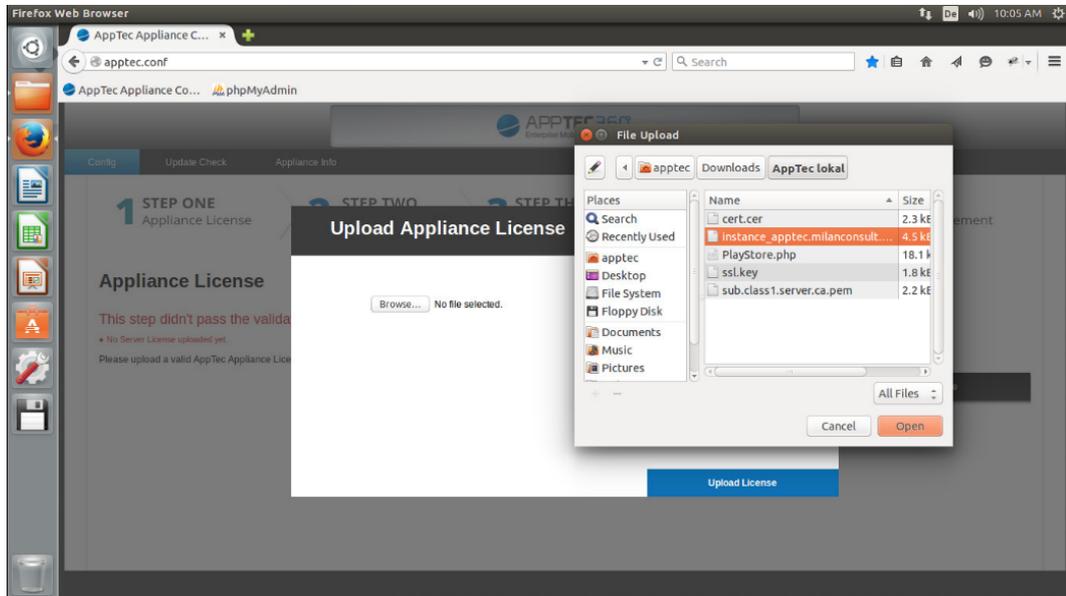
- Laden Sie Ihre Lizenzdatei die Sie von uns erhalten haben, Ihr SSL Zertifikat, Ihren Private Key und Ihre Intermediate Cert Datei die Sie von Ihrer Zertifizierungsstelle erhalten haben z.B. auf Ihrem FTP / SFTP Server hoch. Dies kann allerdings auch per SSH kopiert werden.
- Öffnen Sie anschließend einen neuen Tab im Firefox (VM) und tragen Sie als URL Ihren FTP Server ein.
- Sie werden aufgefordert Ihren Usernamen und Passwort einzutragen.



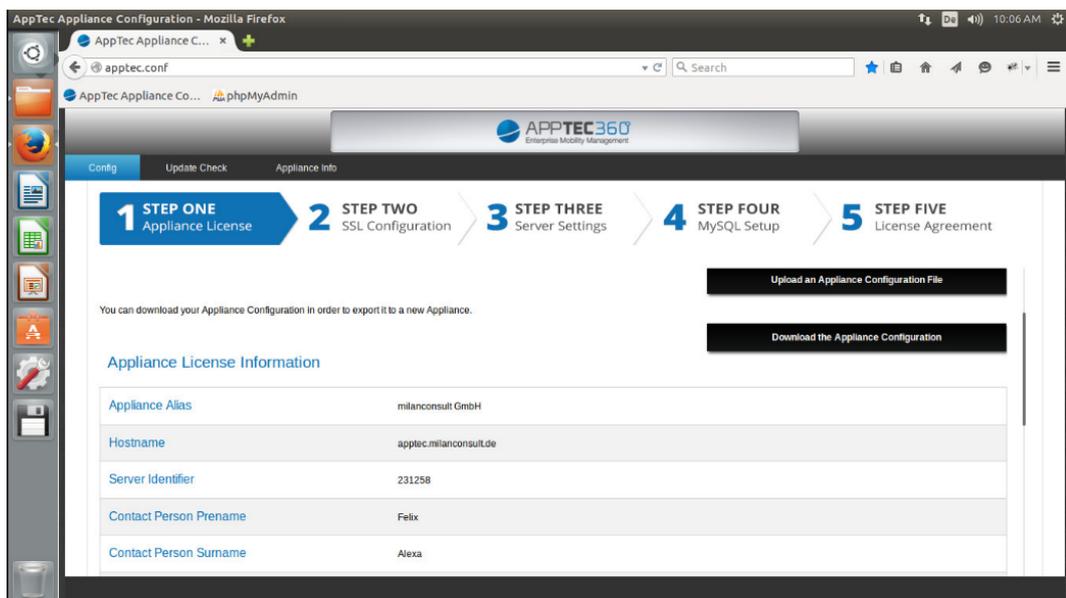
- Anschließend laden Sie sich Ihre Lizenzdatei, das SSL Zertifikat, den Private Key und Ihr Intermediate Cert herunter.
- Öffnen Sie im Nachgang folgende URL „apptec.conf“

➤ „STEP ONE – Appliance License“

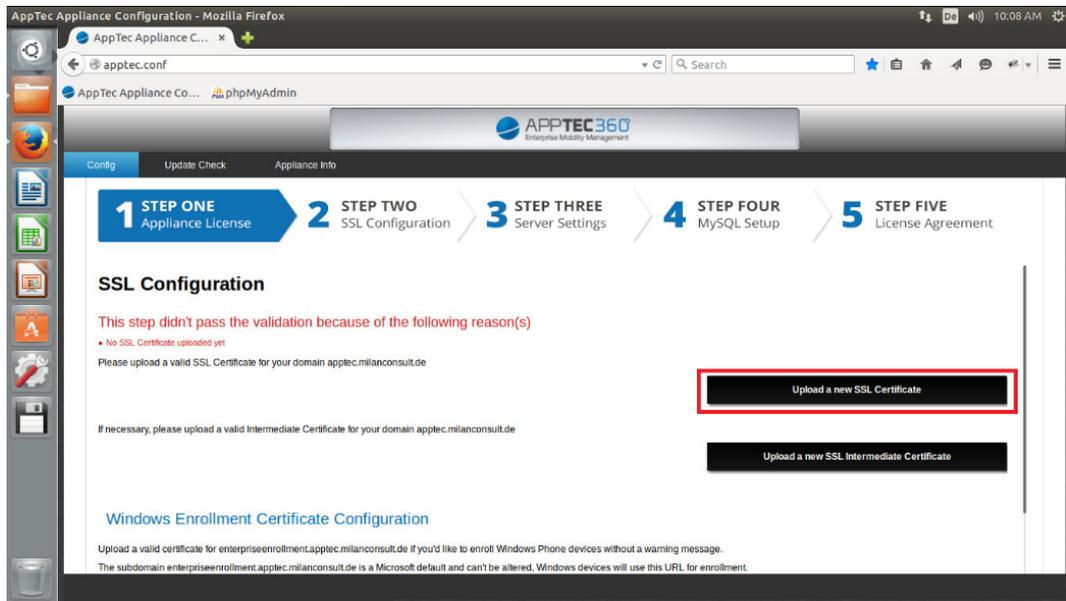
- Klicken Sie auf „Upload an Appliance Configuration File“, navigieren Sie zu der Lizenzdatei die Sie vorhin gespeichert haben und öffnen Sie diese.



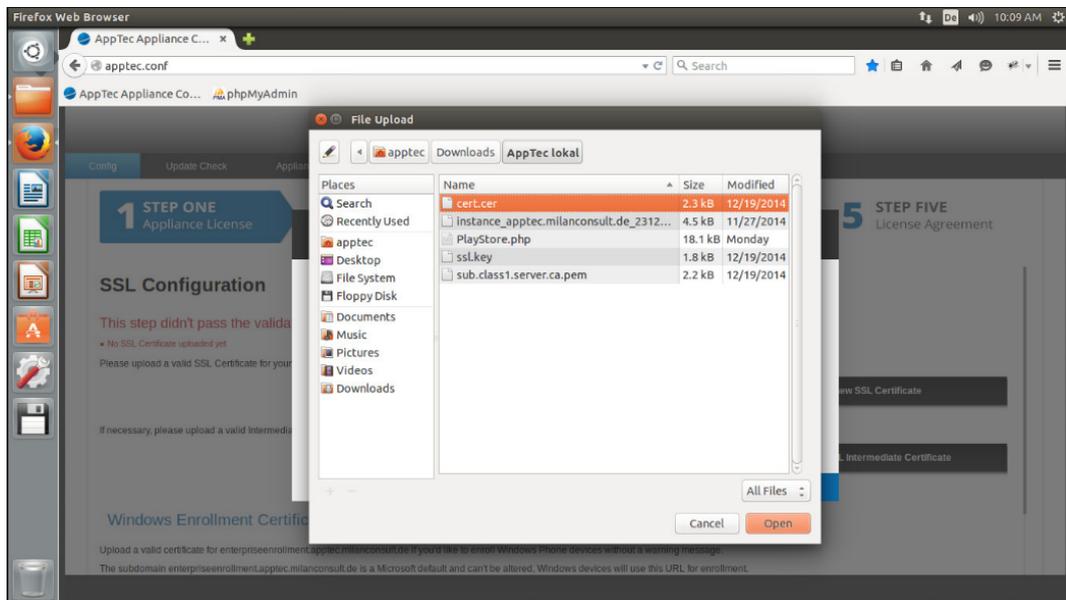
- Sollte dies erfolgreich gewesen sein sollten Sie folgende Ansicht sehen (mit Ihren Daten)



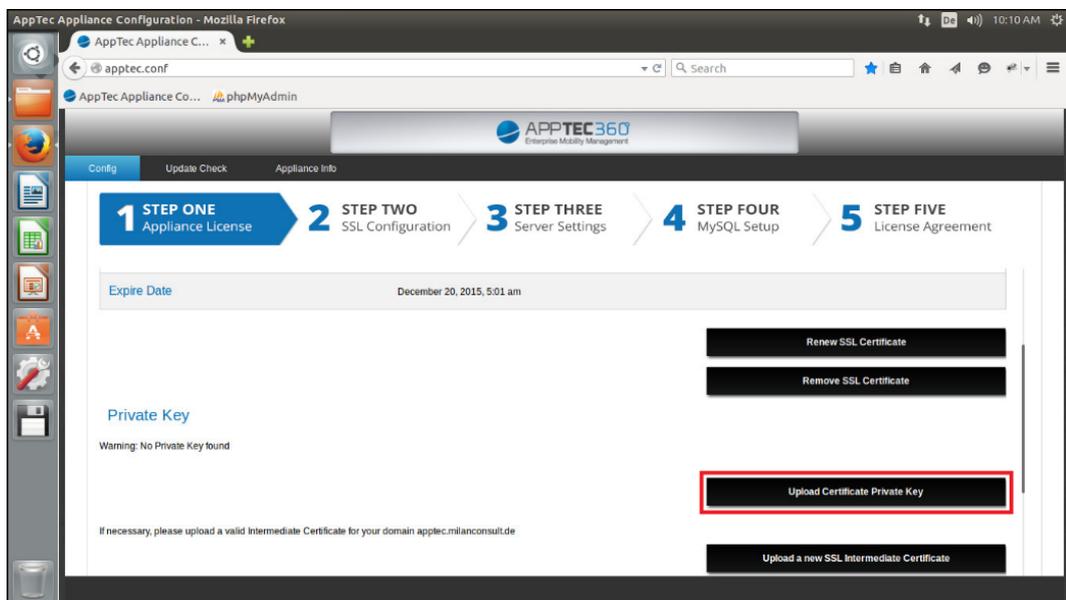
- „STEP TWO – SSL Configuration“
 - Klicken Sie auf „Upload a new SSL Certificate“.



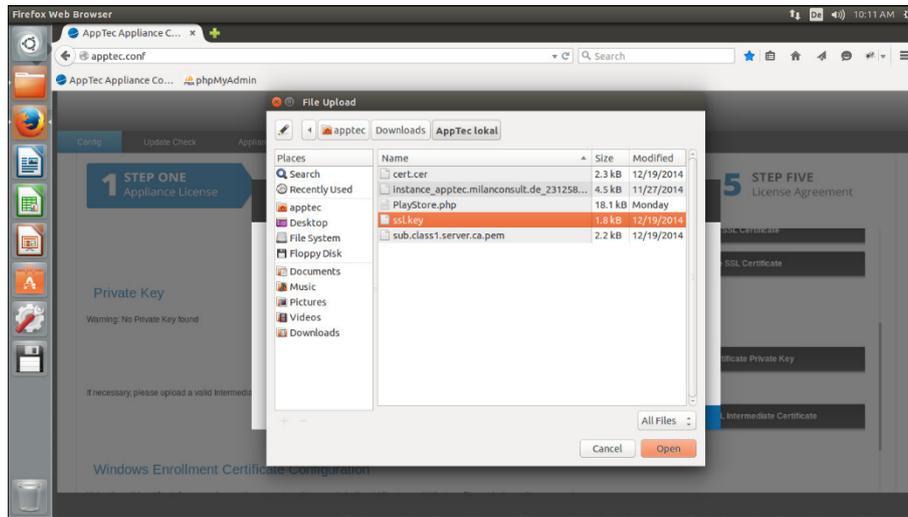
- Navigieren Sie zu Ihrem Speicherort des SSL Zertifikats, wählen Sie dieses aus und klicken Sie auf „Open“.



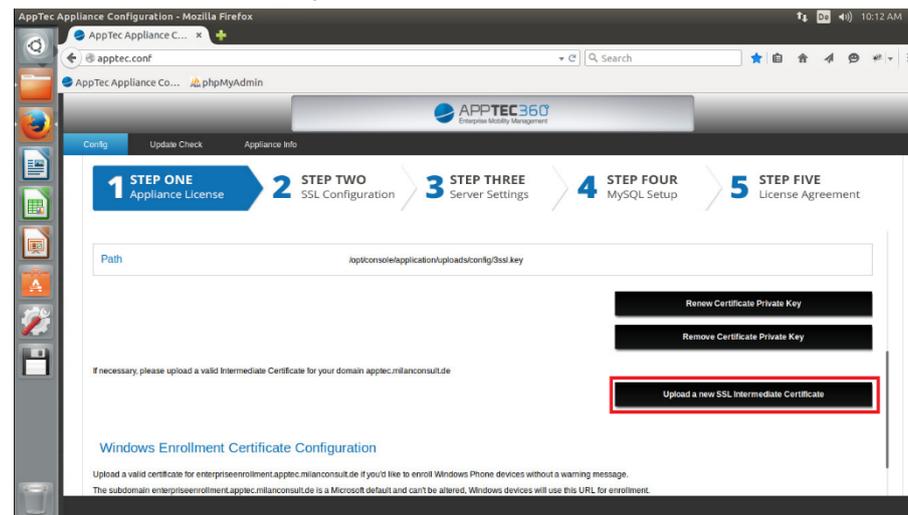
- Klicken Sie nun auf „Upload Certificate Private Key“
Hinweis: Der Private Key darf nicht passwortgeschützt sein!



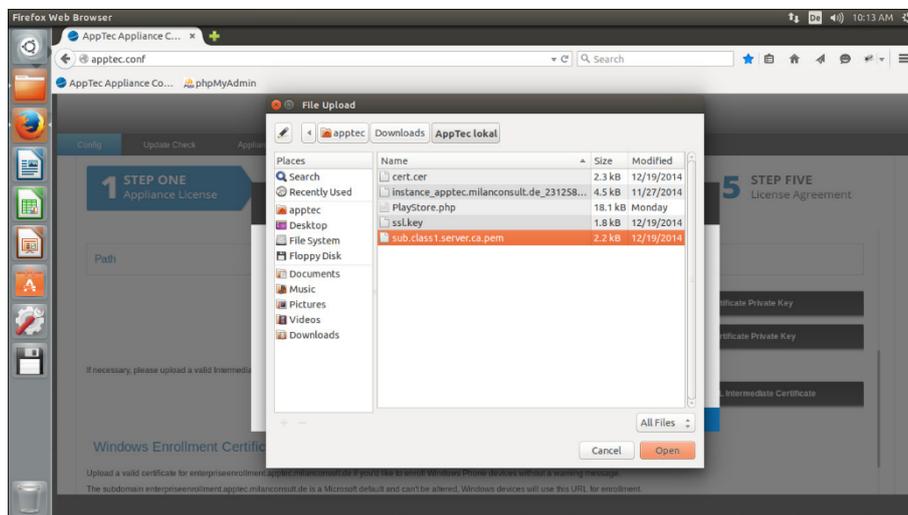
- Navigieren Sie erneut zu Ihrem Speicherort, wählen Sie den Private Key aus und klicken Sie auf „Open“.



- Klicken Sie auf „Upload a new SSL Intermediate Certificate“

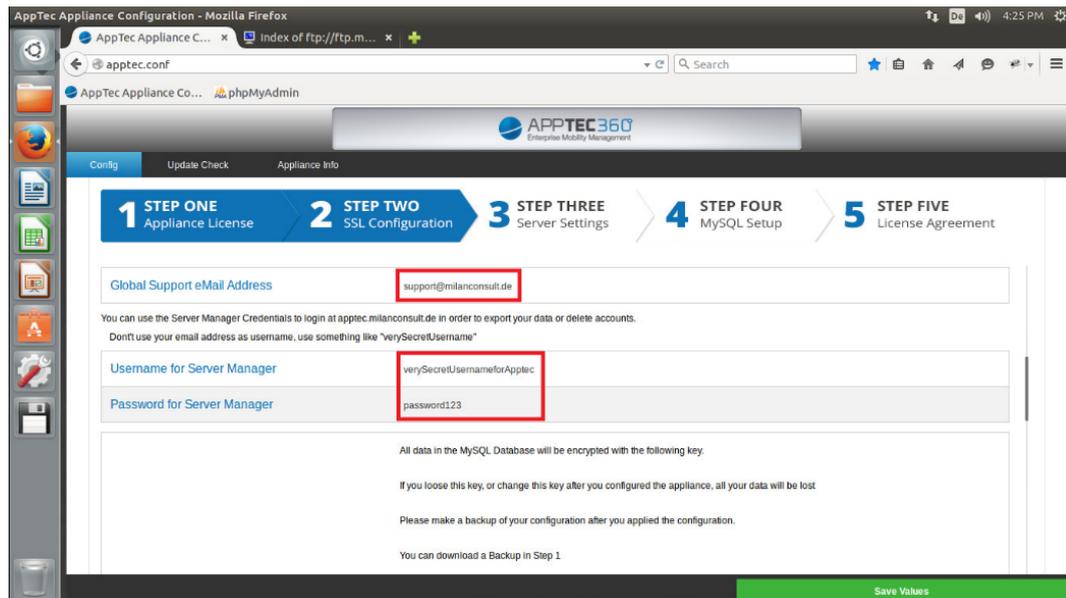


- Navigieren Sie zu Ihrem Speicherort, wählen Sie die Intermediate Cert aus und klicken Sie anschließend auf „Open“.



➤ „STEP THREE – Server Settings“

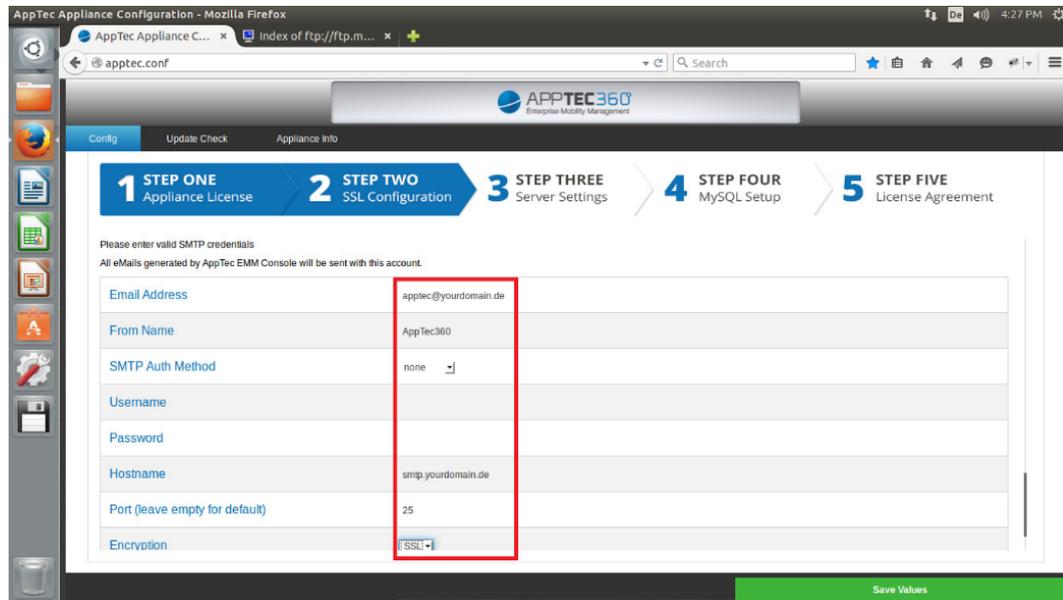
- Bei „Global Support eMail Address“ kann eine Email Adresse angegeben werden, an welche die „Passwort zurücksetzen“ Anfragen gesendet werden – somit eine E-Mail Adresse an die sich die User wenden können.
- Ebenfalls müssen Sie noch einen Username und Password für den Server Manager festlegen.



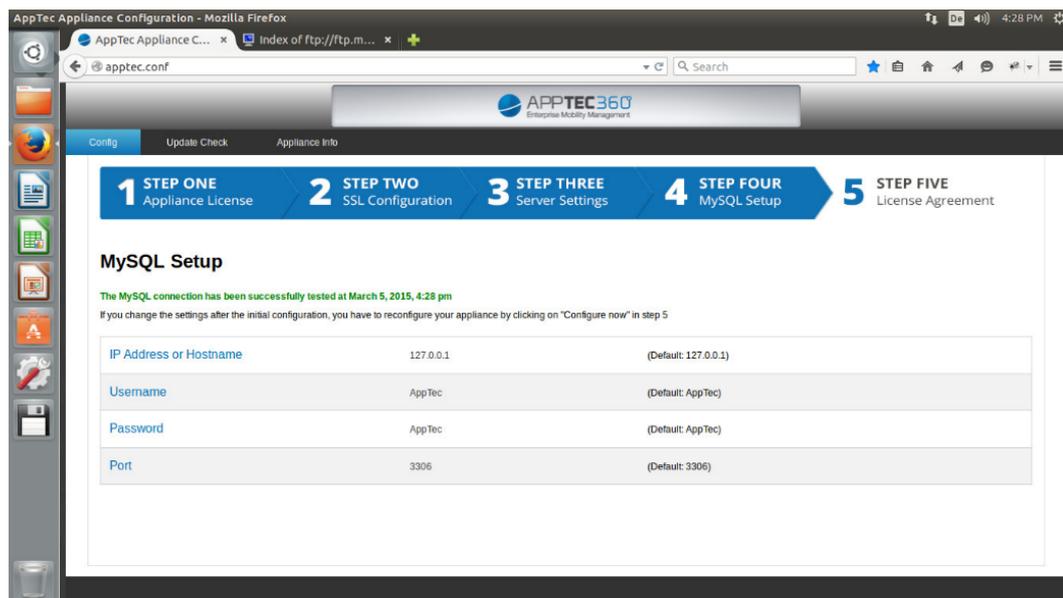
Im Server Manager können Sie folgende Informationen einsehen:

- Company Name
- Registration Date
- License Type
- License Expiration Date
- Account Status
- Devices
- Contact Person
- Phone
- eMail
- Client Identifier
- Database Name
- Root User
- Root Login
- ContentBox
- ContentBox Quota
- **Ebenfalls kann mit „Export Client Data“ ein Backup des Systems erstellt werden.**

- Wenn Sie weiter nach unten scrollen, finden Sie die Einstellungsmöglichkeiten des SMTP Servers, dieser dient dazu, dass AppTec in der Lage ist E-Mails zu versenden, **ohne** einen SMTP Server können Sie sich nicht bei AppTec anmelden und somit AppTec nicht nutzen!
Konfigurieren Sie deshalb nun bitte den SMTP Server.

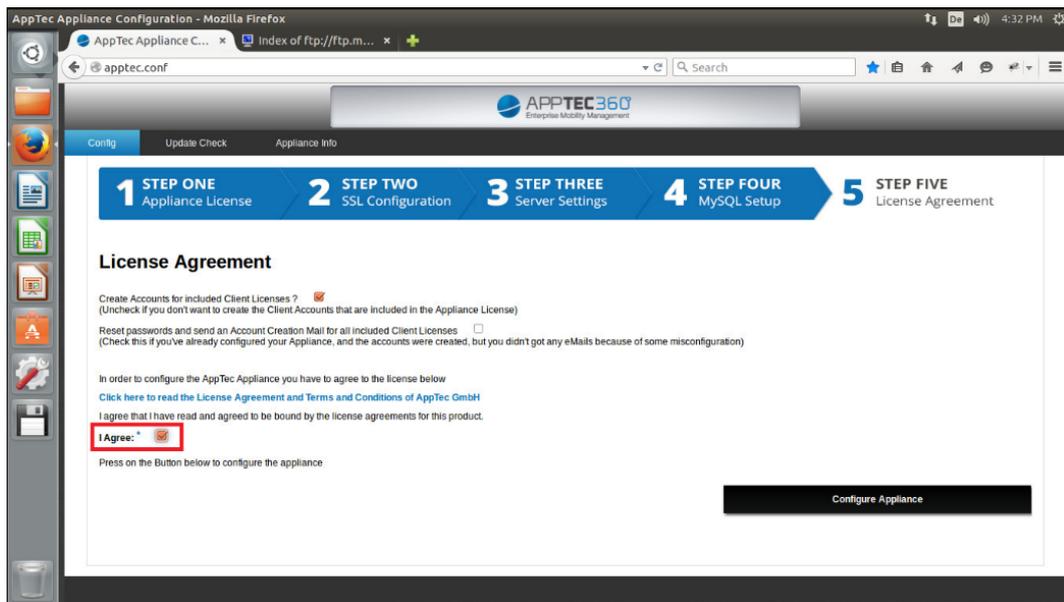


- „STEP FOUR – MySQL Setup“
 - Hier können Sie die MySQL Daten nach Ihren Wünschen anpassen, sollten Sie diese Einstellung nicht ändern möchten, können Sie direkt zu „STEP FIVE“.



➤ „STEP FIVE – Licence Agreement“

- Vergewissern Sie sich dass der Haken bei „Create Accounts for included Client Licenses“ gesetzt wurde!
- Setzen Sie den Haken bei "I Agree" um die AGB's zu akzeptieren. Drücken Sie anschließend auf "Configure Appliance" um die Konfiguration anzuwenden. Dieser Schritt ist muss bei jeder Änderung in der Konfigurationsoberfläche durchgeführt werden.



III. General Settings

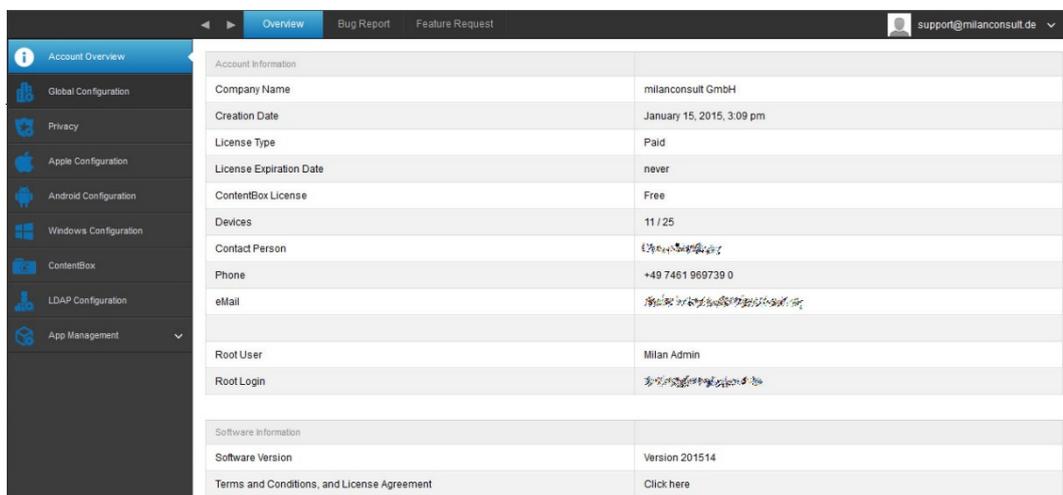
Account Overview

Overview

Hier erhalten Sie einen Überblick über Ihren AppTec Account.

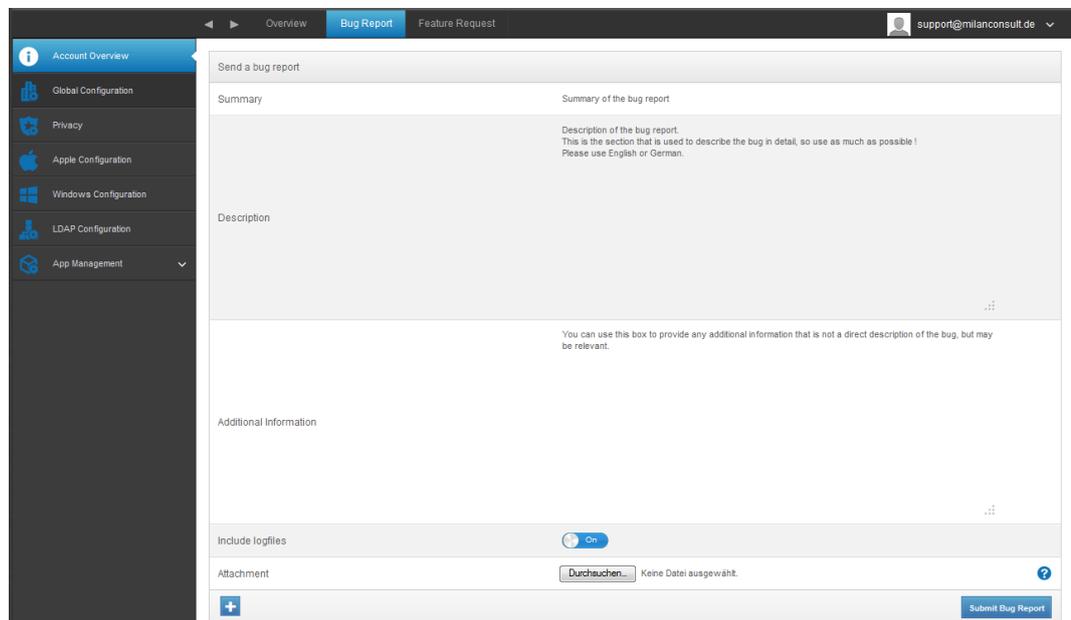
Company Name	Ihr Firmenname
Creation Date	Erstelldatum von AppTec
License Type	Paid = bezahlt Free = kostenlose Lizenz
License Expiration Date	Ablaufdatum Ihrer AppTec Lizenz
ContentBox License	Free = Kostenlose Lizenz für 25 Geräte Paid = Gekaufte Lizenz für x Geräte
Devices	Wie viel Geräte registriert und noch registriert werden können
Contact Person	angegebene Kontaktperson
Phone	angegebene Telefonnummer
eMail	angegebene Email Adresse
Root User	User auf der EMM Console
Root Login	E-Mail mit der Sie sich auf der EMM Console anmelden
Software Version	aktuelle Software Version
Terms and Conditions, and License Agreement	Allgemeine Geschäftsbedingungen (Weiterleitung auf die AppTec Webseite, dort finden Sie diverse PDF Dateien hierzu)

ug
Rep
ort



ie Weboberfläche kann direkt ein Bug Report an den Support geschickt werden.

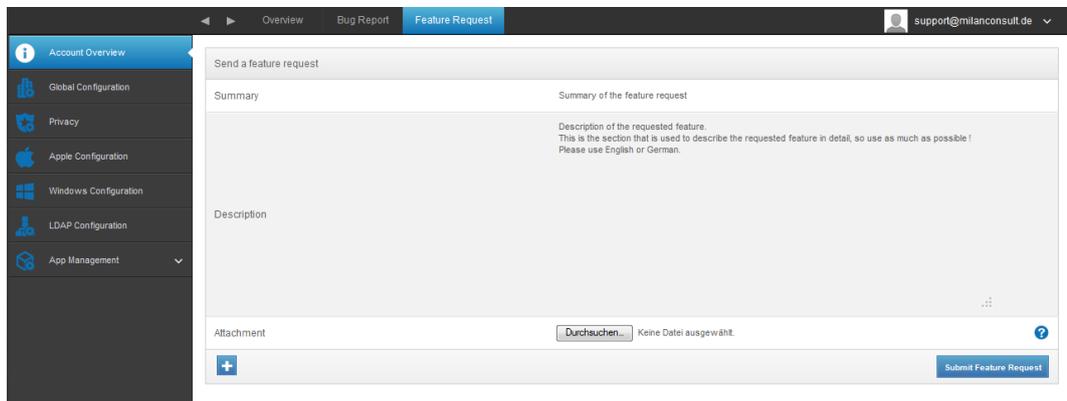
Summary	Eine kurze Zusammenfassung Ihres Problems
Description	Eine ausführliche Beschreibung Ihres Problems, bitte so detailliert wie möglich
Additional Information	Zusätzliche Informationen die nicht direkt das Problem beschreiben, ggf. jedoch nützliche sein könnten
Include logfiles	Möglichkeit die Logdateien direkt mitzusenden
Attachment	Dem Bugreport einen Anhang mitgeben
,blaues Plusymbol‘	Für zusätzliche Anhänge
Submit Bug Report	Bug Report abschicken



Feature Request

Über die Weboberfläche kann auch direkt ein Feature Request an den Support geschickt werden.

Summary	Eine kurze Zusammenfassung Ihres Problems
Description	Eine ausführliche Beschreibung Ihres Problems, bitte so detailliert wie möglich
Attachment	Dem Bugreport einen Anhang mitgeben
‚blaues Plussymbol‘	Für zusätzliche Anhänge
Submit Feature Request	Feature Request abschicken



The screenshot shows the 'Feature Request' form in the AppTec360 web interface. The form is titled 'Send a feature request' and includes the following sections:

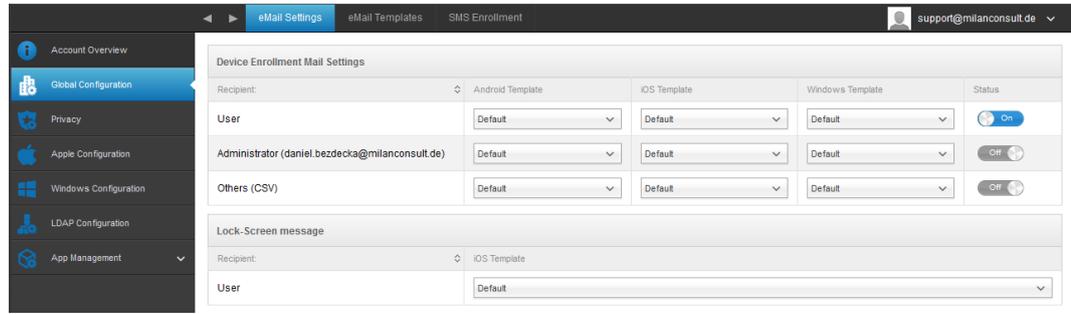
- Summary:** A text area for providing a short summary of the feature request.
- Description:** A larger text area for providing a detailed description of the requested feature. A note below the field states: 'Description of the requested feature. This is the section that is used to describe the requested feature in detail, so use as much as possible! Please use English or German.'
- Attachment:** A section for adding files, currently showing 'Keine Datei ausgewählt' (No file selected) and a 'Durchsuchen...' (Browse...) button.
- Submit Feature Request:** A blue button at the bottom right to submit the request.

The left sidebar contains navigation options: Account Overview, Global Configuration, Privacy, Apple Configuration, Windows Configuration, LDAP Configuration, and App Management.

Global Configuration

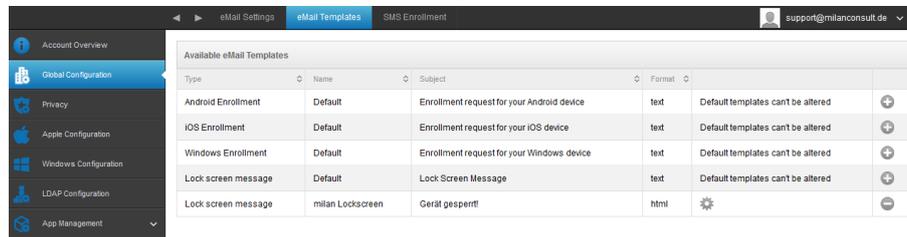
eMail Settings

Hier können die Templates für die jeweiligen Szenarien und Betriebssysteme festgelegt werden.



eMail Templates

Hier sind Sie in der Lage verschiedene Templates für unterschiedliche Szenarien anzulegen, wie z.B. für den Lock Screen (Sperrbildschirm) oder auch die allgemeine E-Mail für das Rollout.

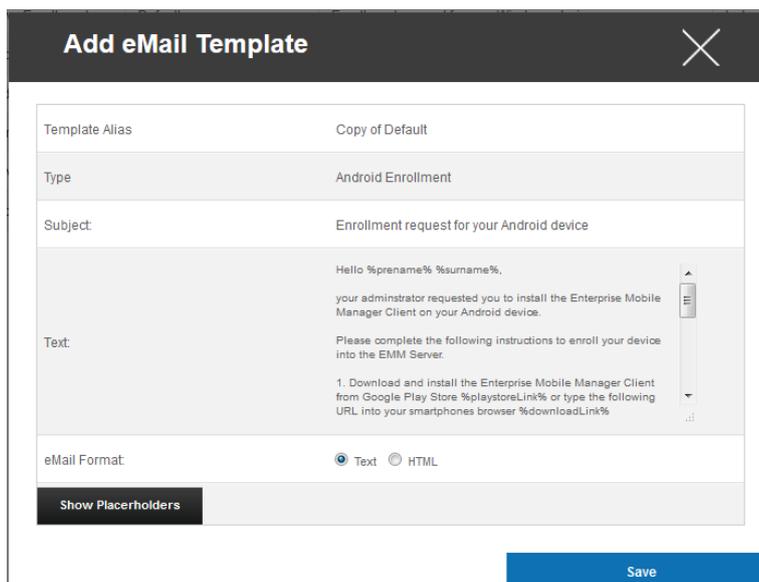


Type	Name	Subject	Format	
Android Enrollment	Default	Enrollment request for your Android device	text	Default templates can't be altered +
iOS Enrollment	Default	Enrollment request for your iOS device	text	Default templates can't be altered +
Windows Enrollment	Default	Enrollment request for your Windows device	text	Default templates can't be altered +
Lock screen message	Default	Lock Screen Message	text	Default templates can't be altered +
Lock screen message	milian Lockscreen	Gerät gesperrt!	html	⚙️ -

Die Default Templates können nicht bearbeitet oder gelöscht werden.

Über das „Plus Symbol“ hinter des jeweiligen Standard Templates können zusätzliche Templates angelegt werden.

Mit dem  Symbol können Sie eine Änderung am Template vornehmen.



Add eMail Template
✕

Template Alias: Copy of Default

Type: Android Enrollment

Subject: Enrollment request for your Android device

Text:

Hello %prenamename% %surname%,
 your administrator requested you to install the Enterprise Mobile Manager Client on your Android device.
 Please complete the following instructions to enroll your device into the EMM Server.
 1. Download and install the Enterprise Mobile Manager Client from Google Play Store %playstoreLink% or type the following URL into your smartphones browser %downloadLink%

eMail Format: Text HTML

[Show Placeholders](#)

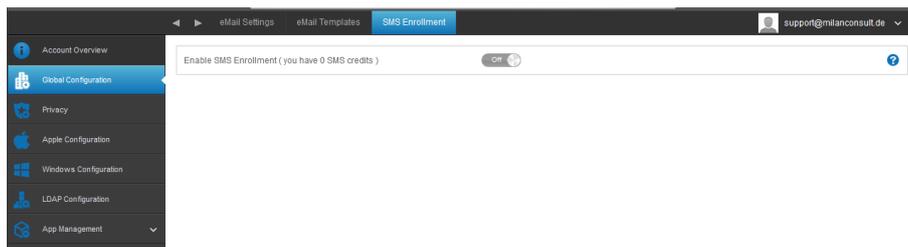
[Save](#)

Ein Beispiel könnte wie folgt aussehen:

SMS Enrollment

Hier können Sie das SMS Enrollment Verfahren de- bzw. aktivieren.
(Standard: deaktiviert)

Ebenfalls wird Ihnen hier angezeigt, wie viel SMS Credits noch verfügbar sind.

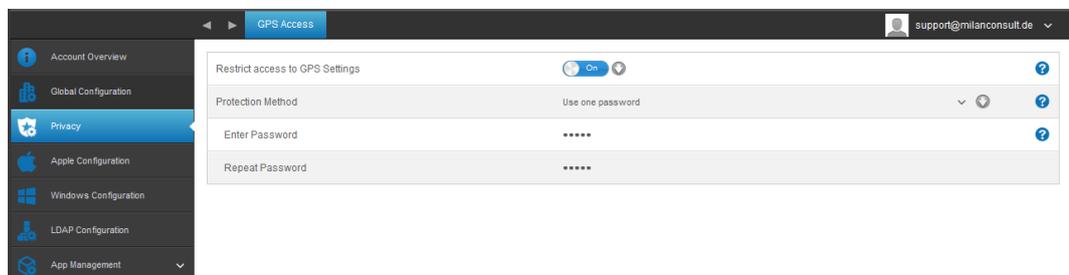


Privacy

GPS Access

Unter “GPS Access” können Sie die Lokalisierung eines Gerätes mit ein oder sogar zwei Passwörtern versehen z.B. für Betriebsrat und IT Abteilung – „vier-Augen-Prinzip“.

Restrict access to GPS Settings	Off = Funktion ist ausgeschaltet und es wird kein Passwort zur Lokalisierung benötigt
	On = Funktion ist angeschaltet und es wird ein Passwort zur Lokalisierung benötigt
Protection Method	Use one password = Ein Passwort zur Lokalisierung benötigt
	Use two passwords = Zwei Passwörter zur Lokalisierung werden benötigt
Enter Password (1)	Gewähltes Passwort eintragen
Repeat Password (1)	Gewähltes Passwort nochmals eintragen
optional: Enter Password 2	2. gewähltes Passwort eintragen
optional: Repeat Password 2	2. gewähltes Passwort nochmals eintragen



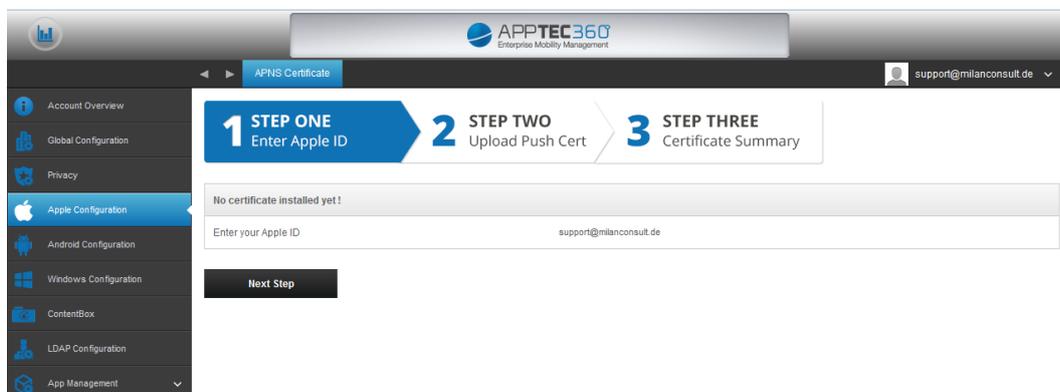
Apple Configuration

APNS Certificate

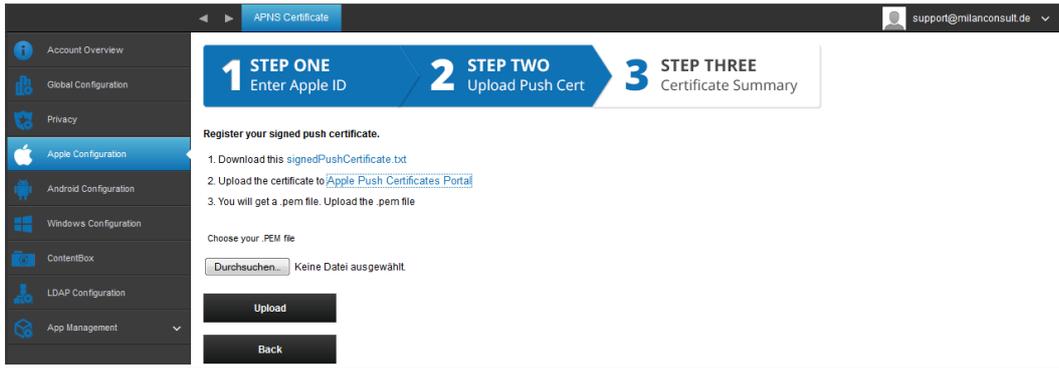
Hier können Sie ein APNS Zertifikat hochladen und verwalten – dieses Zertifikat ist notwendig, damit eine Kommunikation zwischen AppTec und der iOS Endgeräte stattfinden kann.

Hinweis: Diese Prozedur muss jedes Jahr erneut getätigt werden, da das APNS Zertifikat nur ein Jahr gültig ist.

Es muss dann dieselbe Apple ID verwendet werden, ansonsten ist ein zukünftiges Verwalten der iOS Geräte nicht mehr möglich und alle Geräte müssen neu eingerollt werden.

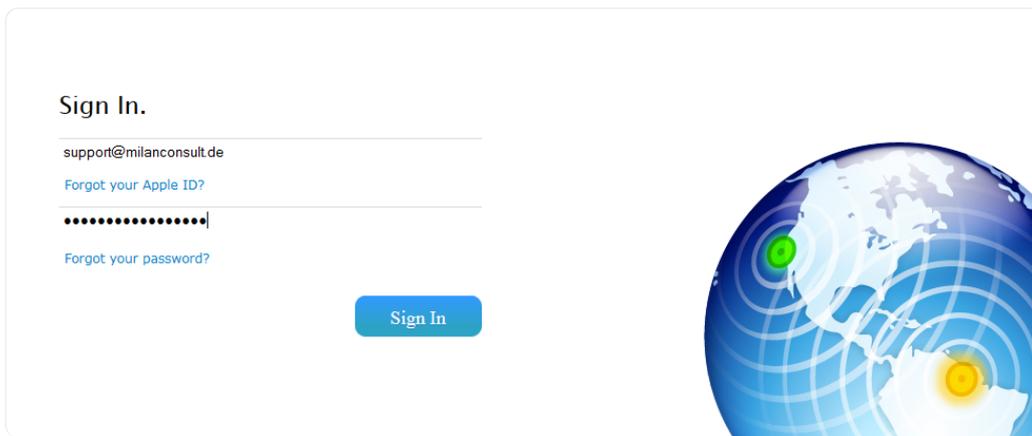


- Geben Sie zuerst Ihre Apple ID ein und klicken Sie auf „Next Step“ (Empfehlung: Es sollte sich hierbei um eine generische Apple ID handeln)
- Laden Sie sich anschließend die „signedPushCertificate.txt“ Datei herunter indem Sie darauf klicken.
- Klicken Sie anschließend auf „Apple Push Certificates Portal“, Sie sollten nun an folgende URL weitergeleitet werden:
<https://identity.apple.com/pushcert/>



- Melden Sie sich nun bitte mit Ihrem Apple Account an.

Apple Push Certificates Portal

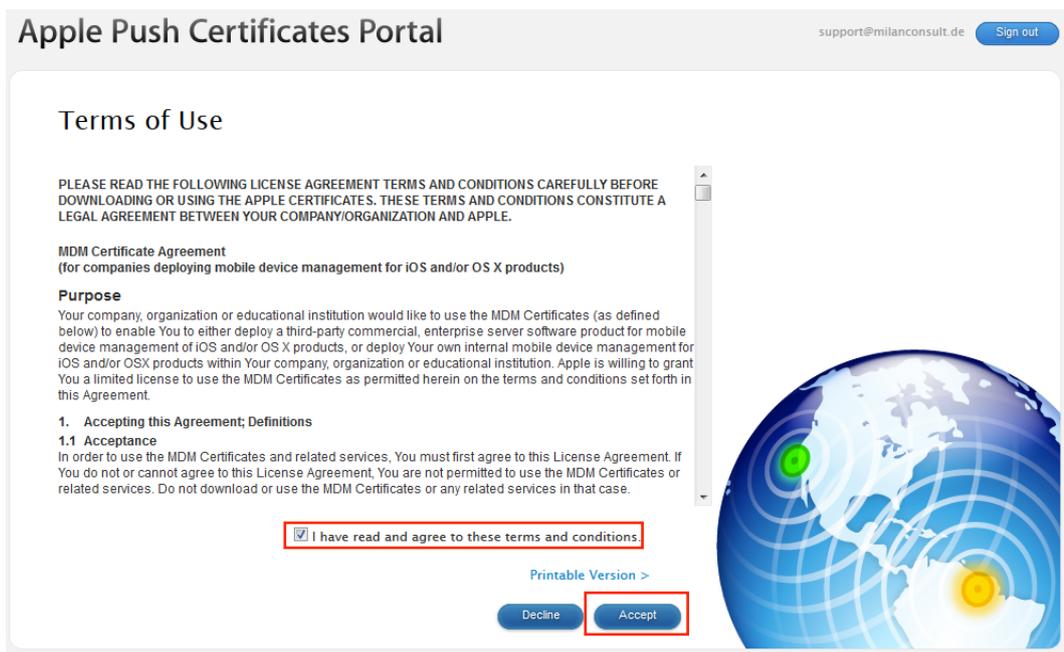


- Klicken Sie, sobald Sie sich erfolgreich anmelden konnten, auf „Create a new Certificate“.

Certificates for Third-Party Servers



- Akzeptieren Sie die Allgemeinen Geschäftsbedingungen



Klicken Sie auf „Durchsuchen...“ und wählen Sie das von Ihnen vorher erstellte „signedPushCertificate.txt“ aus.

- Schreiben Sie sofern erwünscht (für eine evtl. spätere Zuordnung) etwas Aussagekräftiges in die „Notes“.
- Klicken Sie anschließend auf „Upload“.

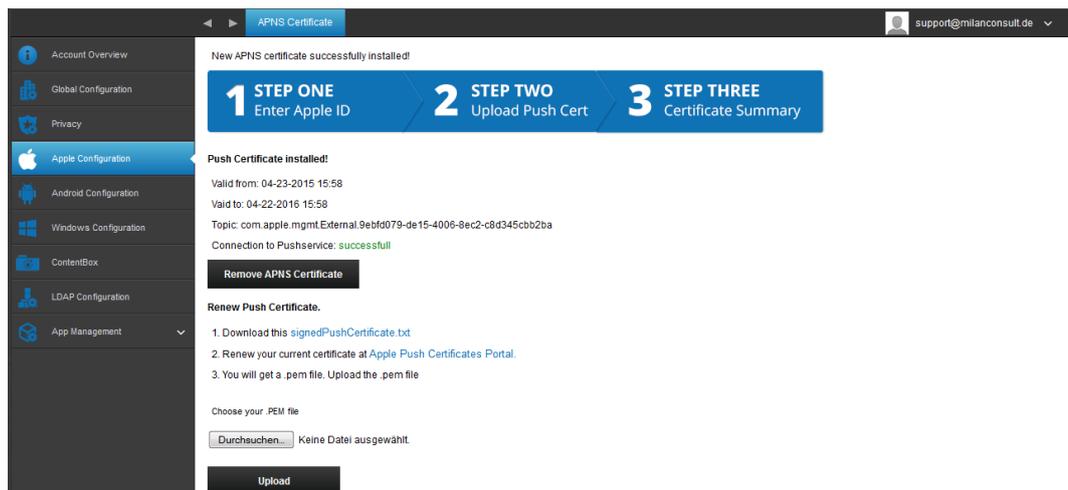
- Im Nachgang sollten Sie folgende Ansicht erhalten

- Klicken Sie auf „Download“

- Gehen Sie nun wieder zurück auf die AppTec Console und wählen nun unterhalb von „Choose your .PEM file“ „Durchsuchen...“ aus.
- Wählen Sie nun die eben heruntergeladene Datei aus und klicken Sie anschließend auf „Upload“.



- Sollte diese Prozedur erfolgreich gewesen sein, erhalten Sie nun folgende Ansicht – nun können Sie Apple Geräte enrollen und verwalten.



Android Configuration

Android Configuration

<p>Uninstall Protection</p>	<p>Falls diese Funktion aktiviert ist, kann der User den Geräteadministrator nicht ohne das vom Admin festgelegte Passwort deaktivieren Für das Entfernen des Geräteadministrators gibt es zwei verschiedene Varianten:</p> <ul style="list-style-type: none"> a. Die Manuelle (Endgerät) <ul style="list-style-type: none"> → EMM App auf dem Endgerät öffnen → Status → Uninstall Protection anklicken → Passwort eingeben b. Die Automatische (Console) <ul style="list-style-type: none"> → Enterprise Wipe durchführen <p>Hinweis: Nur bei Android 4.x und niedriger oder mit Geräten mit der SAFE API verfügbar</p>
<p>Uninstall Password (Revision x)</p>	<p>Das festgelegte Passwort, womit der User den Geräteadministrator entfernen kann Revision x = Zähler, wie oft das Passwort bereits verändert wurde Wichtig welches Passwort der User benötigt, da evtl. das Gerät sich seit einer gewissen Zeit nicht mehr beim AppTec Server gemeldet hat und somit das aktuellste Passwort noch nicht übertragen wurde</p>
<p>Password History</p>	<p>Wenn Sie auf den blauen Button klicken („Show History“), sind Sie in der Lage alle bereits definierten Passwörter einzusehen</p>
<p>Extended Uninstall Protection</p>	<p>Diese Option bietet einen Schutz für nicht-SAFE Geräte Sofern diese Einstellung aktiviert ist, ist es nicht möglich den Geräte Administrator ohne weiteres zu deaktivieren</p>



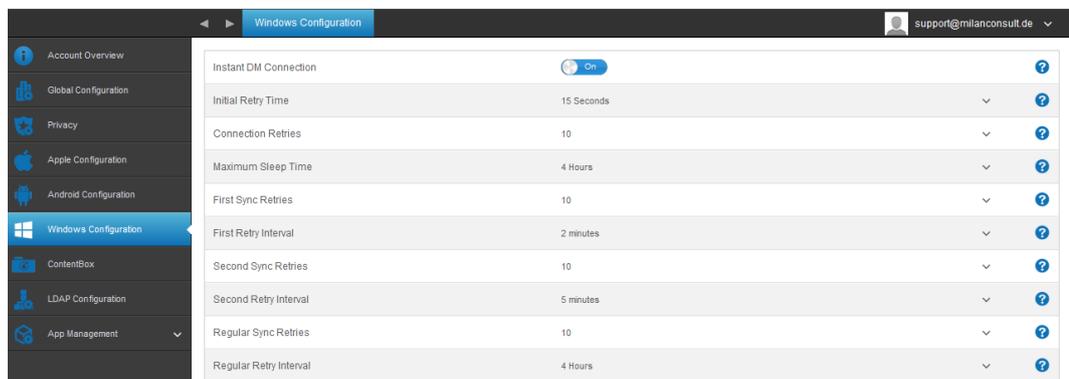
Windows Configuration

Windows Configuration

Hier sind Sie in der Lage folgende Konfigurationen für Ihr Windows Phone zu tätigen:

Instant DM Connection	
Initial Retry Time	Legt den Intervall für den ersten Verbindungsversuch zum Gerät fest, dieser Wert steigt exponentiell
Connection Retries	Gibt an, wie viel Verbindungsversuche der DM-Client unternehmen soll bei einem Verbindungsfehler
Maximum Sleep Time	Gibt die maximale Ruhezeit nach einem Verbindungsfehler an
First Sync Retries	Häufigkeit, wie oft sich das Gerät nach dem ersten einbinden beim Server melden soll
First Retry Interval	Bezieht sich auf „First Sync Retries“, hier wird die Zeit in Minuten angegeben z.B. wird unter „First Sync Retries“ der Wert „2“ eingetragen und bei „First Retry Interval“ der Wert „4 Minuten“, somit meldet sich das Gerät nach dem ersten Einbinden 2 Mal alle 4 Minuten
Second Sync Retries	Häufigkeit, wie oft sich das Gerät nach Abwicklung des „First Sync Retries“ beim Server melden soll

Second Retry Interval	Selbes Prinzip wie für „First Retry Interval“ – nur dass es hier selbstverständlich für „Second Sync Retries“ gilt
Regular Sync Retries	Häufigkeit, wie oft sich das Gerät für die Zukunft am Server melden soll Standard: „Infinite“ Wir empfehlen diesen Wert nicht zu ändern, falls Sie hier nämlich z.B. „10“ eintragen, wird sich das Gerät 10x am Server melden und anschließend nicht mehr Somit bricht eine Verbindung zum AppTec Server ab!
Regular Retry Interval	Selbes Prinzip wie für „First/Second Retry Interval“ – nur dass es sich hierbei um die Einstellung für die Zukunft handelt



Content Box

Configuration

Unter diesem Punkt können Sie die ContentBox konfigurieren.

Die ContentBox können Sie sich wie eine Enterprise Dropbox vorstellen.

Enable ContentBox	ContentBox aktivieren
Use external ContentBox installation	Die ContentBox kann ebenfalls mit ihrem eigenen ownCloud 7 Server betrieben werden
URL	Vollständige URL der OwnCloud Instanz
Root User	Root User des owncloud Accounts
Root Password	Root Passwort des ownCloud 7 Accounts
Default group folder permissions	Standardberechtigung für eine Gruppe, kann individuell je Gruppe geändert werden (im Mobile Management)
Share group folder with subgroups	Wenn aktiv, kann jede Untergruppe alle Ordner der Hauptgruppe lesen, kann ebenfalls individuell für jede Gruppe angepasst werden (Mobile Management)
Permissions for subgroups	Berechtigung für die Untergruppe read = lesen write = schreiben delete = löschen Kann je Gruppe individuell eingestellt werden (Mobile Management)
Allow sharing	Erlaubt es dem User den Inhalt via Links zu teilen, kann individuell für jede Gruppe eingestellt werden
Maximum File Upload Size in MB	Maximale Größe einer Datei Standard: 512 MB Maximal einstellbar: 2048
WebDAV Credentials	
WebDAV URL	Sie können Ihre ContentBox auch mit WebDav aufrufen. Löschen Sie bitte auf keinen Fall folgende Ordner: /apptecgroups /apptecgroups/AppTecGroup-X
Root User	Name des Root Users
Password	Passwort des Root Users

Die Synchronisation mit der ContentBox erfolgt automatisch, Sie können hier aber zusätzlich mit „Synchronize ContentBox“ eine manuelle Synchronisation der ContentBox durchführen.

Ebenfalls können Sie für jedes einzelne Gerät die ContentBox hier deaktivieren bzw. aktivieren.

Dies ist nur dann relevant, wenn Sie die ContentBox nicht zusätzlich lizenziert haben, Ihnen stehen dann dennoch 25 Geräte zur Verfügung um die ContentBox teste zu können – hier können Sie dies für die jeweiligen Geräte aktivieren.

Last synchronization: 2015-06-22 13:49:35

Synchronize ContentBox

You don't have a subscription for the AppTec ContentBox. Your ContentBox access is limited to 25 devices.

Contact sales@apptec360.com to purchase a license for all your devices

Select the 25 devices that can access the ContentBox

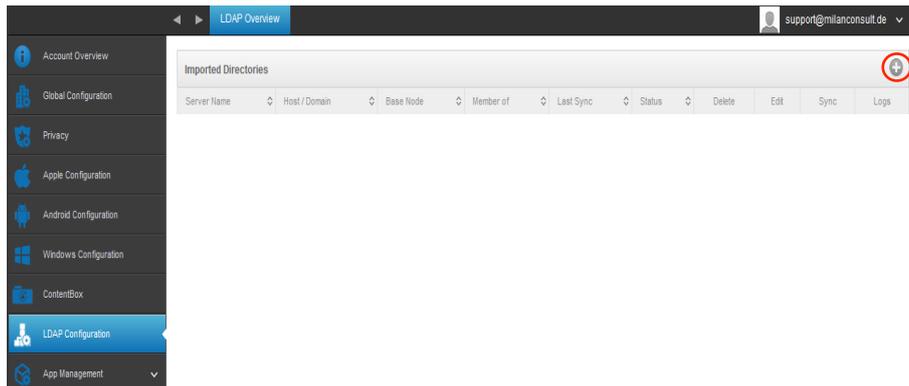
#		Device	OS	Type	Owner
1		Device of Fabian	iOS	Tablet	Fabian Kola
2		Device of Matthias	Android	Phone	Matthias
3		Device of Michael	iOS	Phone	Michael
4		Device of Michael	iOS	Tablet	Michael
5		Device of Martina	iOS	Phone	Martina
6		Device of Yasemin	iOS	Phone	Yasemin
7		Device of Michael	iOS	Phone	Michael
8		Device of Tanja	Android	Phone	Tanja I
9		Device of Fabian	iOS	Tablet	Fabian
10		Device of Lukas	iOS	Tablet	Lukas
11		Device of Daniel	Android	Phone	Daniel
12		Device of Fabian	iOS	Tablet	Fabian

LDAP Configuration

LDAP Overview

Sollte Ihr Active Directory extern erreichbar sein oder Sie sich für die On-Premise Variante von AppTec entschieden haben, können Sie hier einen LDAP Import vornehmen.

Dies erfolgt über das im Screenshot markierte „Plus Symbol“.



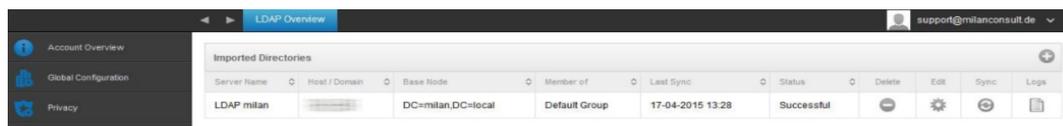
Geben Sie Ihre Active Directory Daten an und klicken Sie auf „Add LDAP Server“:

Add LDAP Server
✕

Server Name		
Type	<input checked="" type="radio"/> Active Directory	
Host Domain		
Host Address		?
Port		?
Username		?
Password		
Repeat password		
Connection Security	<input checked="" type="radio"/> No Encryption <input type="radio"/> Use SSL <input type="radio"/> use TLS	
Base DN		?
Member of	milan	?
Check users for valid eMail ?	<input type="checkbox"/> Off	?
Only activated users?	<input type="checkbox"/> Off	?
Filter by Attributes ?		?
Test connection ?	<input checked="" type="checkbox"/> On	?

Add LDAP Server

Sollte dies erfolgreich gewesen sein, erhalten Sie folgende Ansicht:



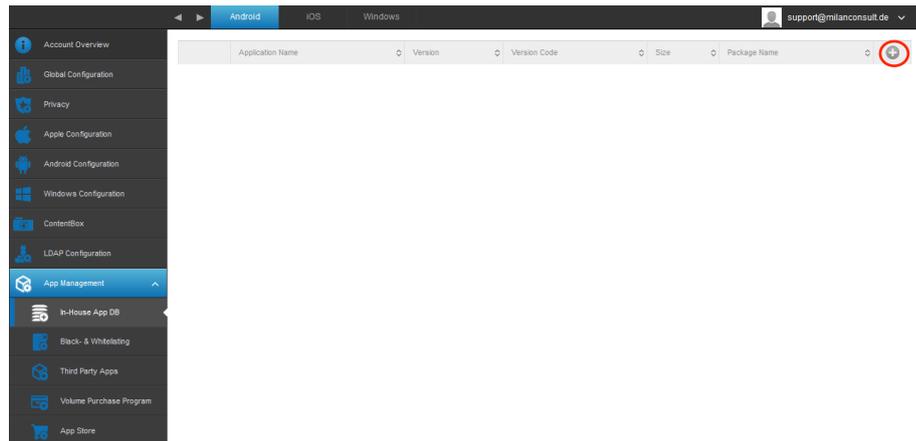
Delete	LDAP Server entfernen
Edit	LDAP Server bearbeiten
Sync	Synchronisation des LDAP Servers
Logs	Ausgabe von LDAP Logs

App Management

In-House App DB

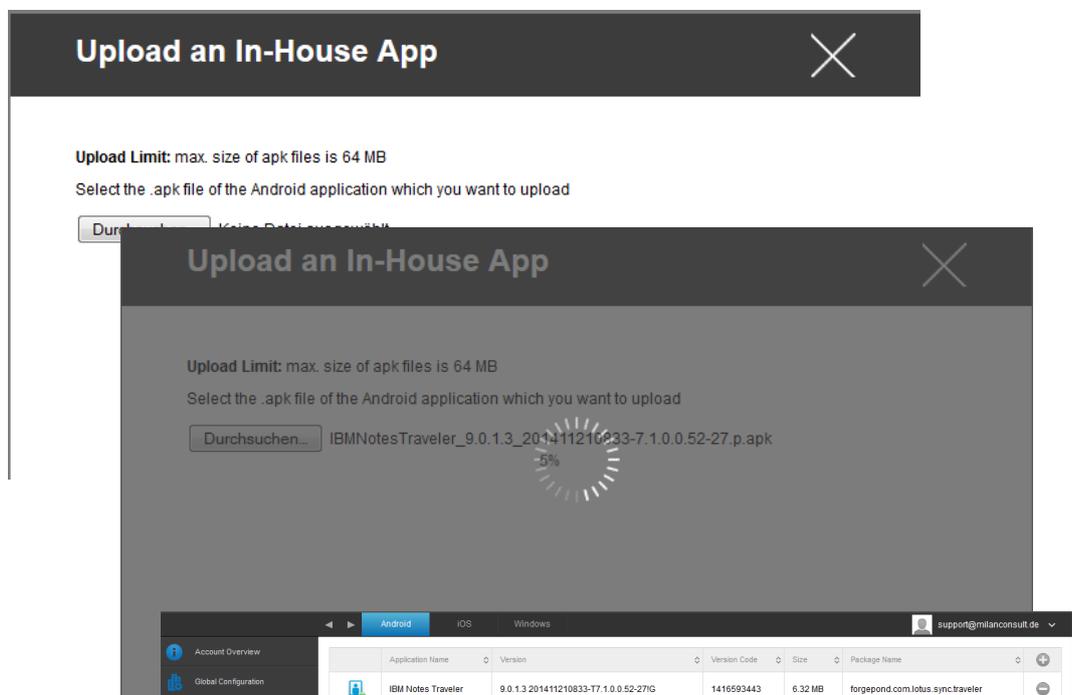
Android

Hier können Sie Ihre eigenentwickelten Android Apps über das „Plus Symbol“ hochladen und später im Mobile Management verteilen.



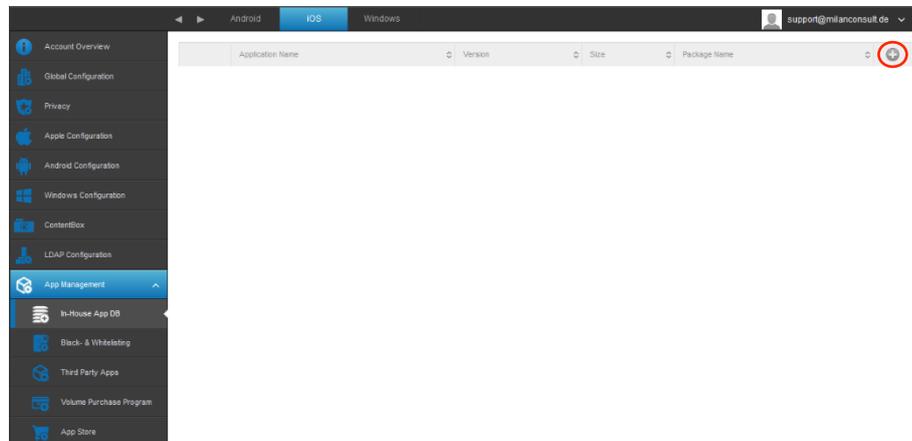
Mit

„Durchsuchen...“ können Sie die .apk Datei auswählen und mit „Upload“ hochladen.

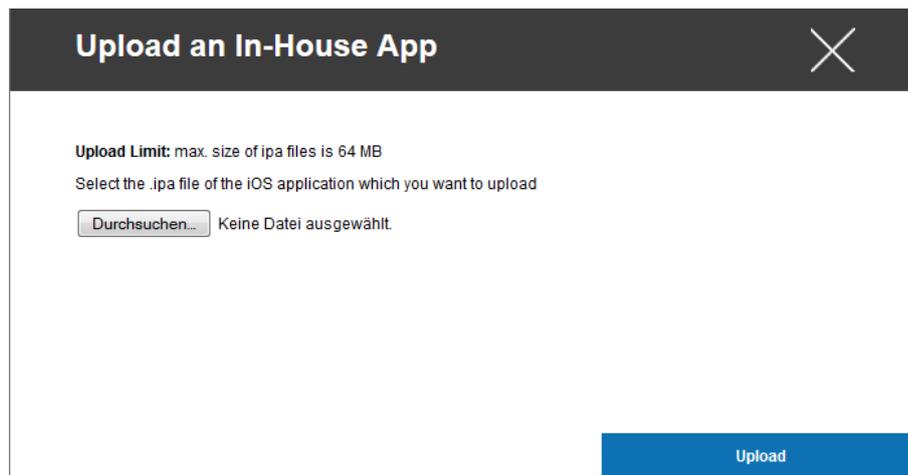


iOS

Hier können Sie Ihre eigenentwickelten iOS Apps über das „Plus Symbol“ hochladen und später im Mobile Management verteilen.

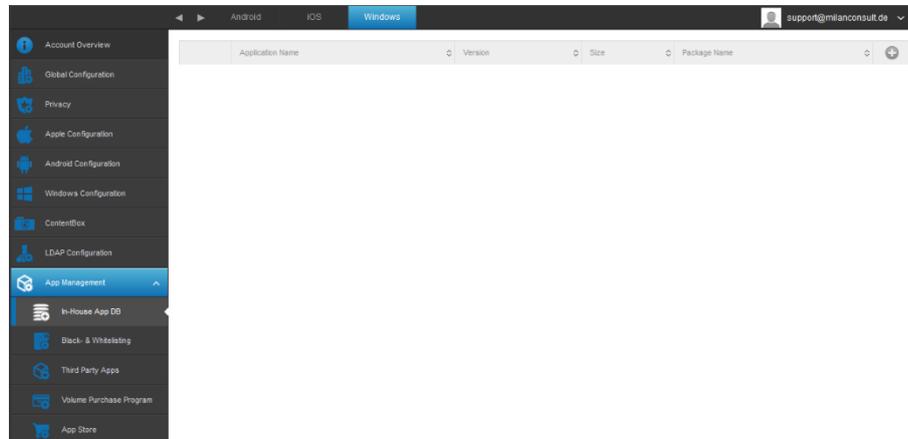


Mit „Durchsuchen...“ können Sie die .ipa Datei auswählen und mit „Upload“ hochladen.

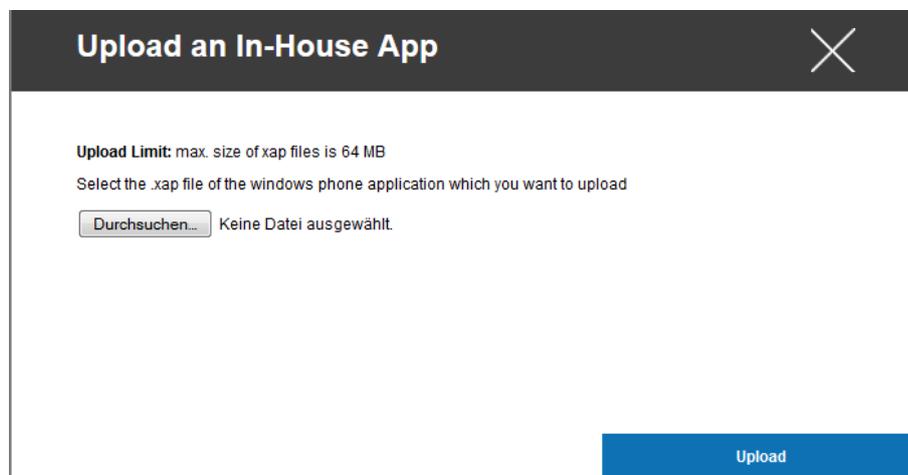


Windows

Hier können Sie Ihre eigenentwickelten Windows Phone Apps über das „Plus Symbol“ hochladen und später im Mobile Management verteilen.



Mit „Durchsuchen...“ können Sie die .xap Datei auswählen und mit „Upload“ hochladen. Diese Dateien müssen jedoch unsigned, ansonsten ist ein Upload nicht möglich.

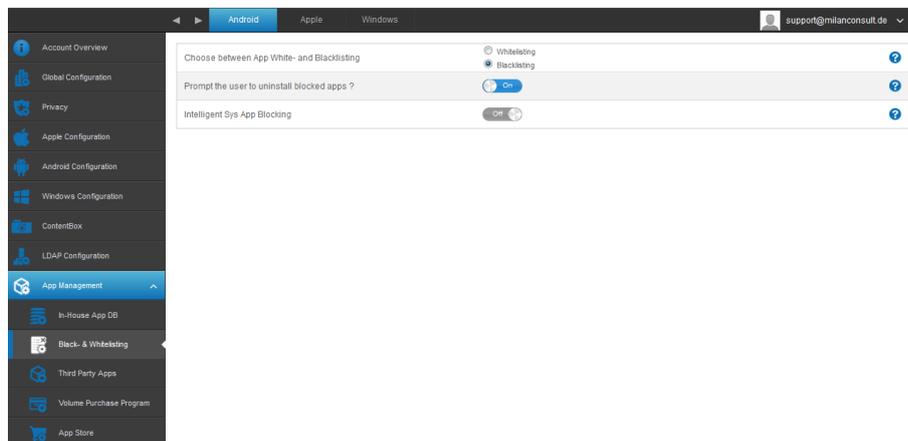


Black-& Whitelisting

Android

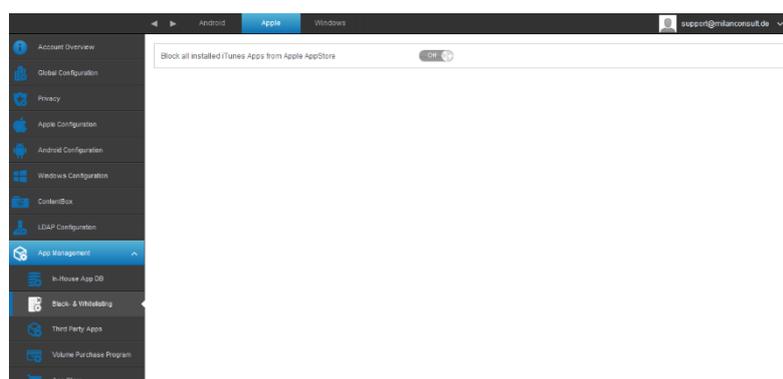
Hier können Sie festlegen, ob Sie mit einem White- oder Blacklisting arbeiten möchten.

Whitelisting	Nur bestimmte Apps sind erlaubt, alle anderen Apps sind nicht installierbar / ausführbar
Blacklisting	Bestimmte Apps sind verboten, alle anderen sind installierbar / ausführbar
Prompt the user to uninstall blocked apps?	Den User dazu auffordern, verbotene Apps zu deinstallieren. Bei SAFE findet dies automatisch statt.
Intelligent Sys App Blocking	Wenn „whitelisting“ aktiviert ist, werden mit dieser Funktion alle System-Apps deaktiviert



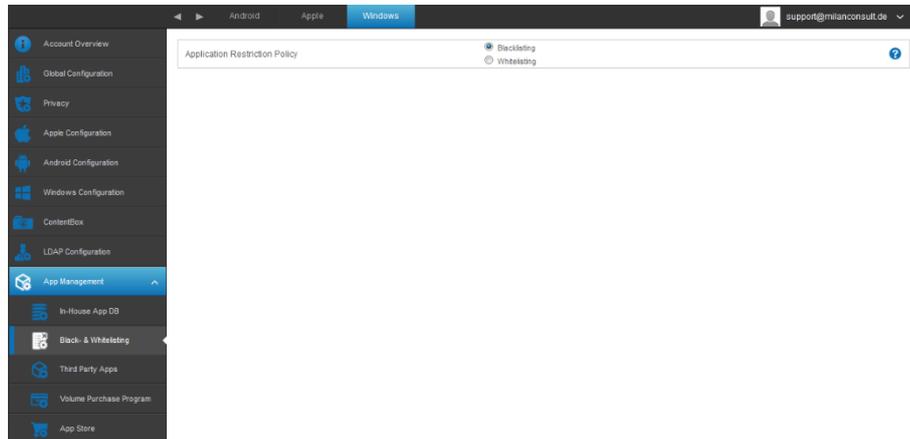
Apple

Block all installed iTunes Apps from Apple AppStore	Alle installierten iTunes Apps werden vom Apple AppStore blockiert / deaktiviert (auch vom MDM installierte Applikationen)
---	--



Windows

Whitelisting	Nur bestimmte Apps sind erlaubt, alle anderen Apps sind nicht installierbar / ausführbar
Blacklisting	Bestimmte Apps sind verboten, alle anderen sind installierbar / ausführbar

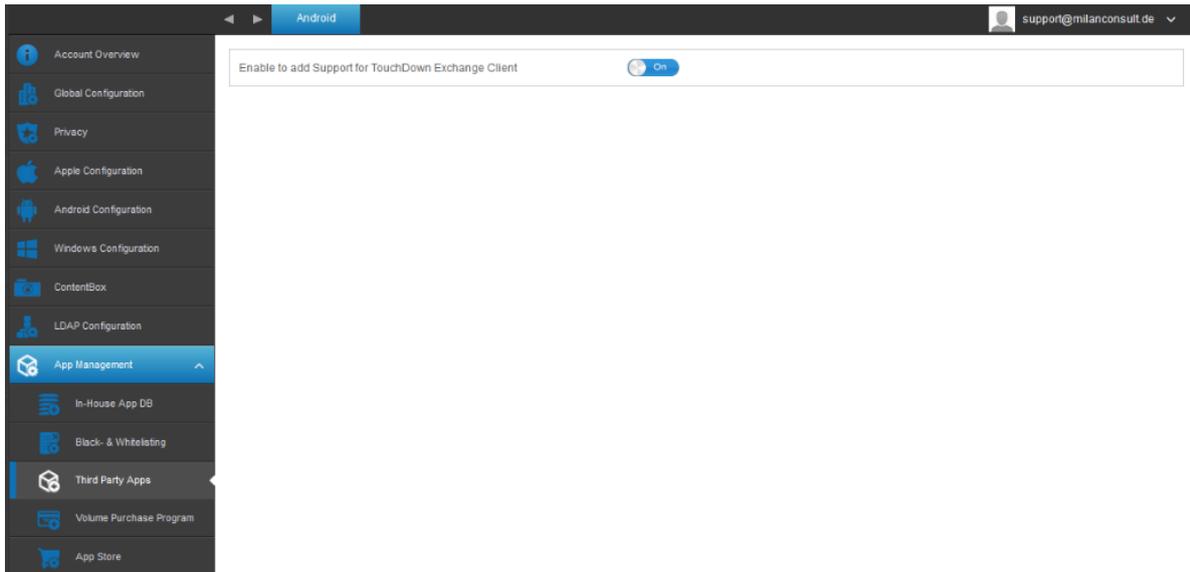


Third Party Apps

Android

Falls der native Mail Client unter Android nicht unterstützt wird, können Sie hier die 3rd Party App "TouchDown" aktivieren.

Diese können Sie anschließend unter „Mobile Management“ > „PIM Management“ > „Touchdown Exchange“ konfigurieren.



VPP / KNOX

Das Volume Purchase Program (VPP) von Apple erlaubt es Ihnen Lizenzen für eine kostenpflichtige App zu erwerben.

Nach dem Erwerb sind Sie in der Lage die Lizenz für bestimmte User zu verteilen, diese können die App dann kostenlos auf dem Endgerät installieren.

Sollte die App auf einem Endgerät deinstalliert werden, bekommen Sie diese Lizenz wieder gut geschrieben und können diese erneut an einen anderen User verteilen.

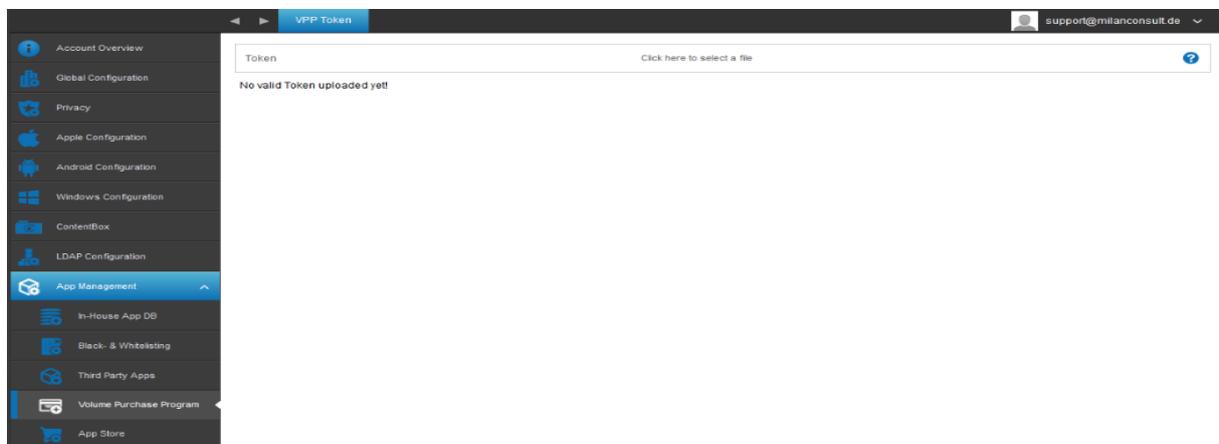
Samsung Geräte können KNOX nutzen, sofern die Geräte es unterstützen und Sie einen gültigen Lizenzschlüssel besitzen.

Mit KNOX können zwei unterschiedliche Profile auf dem Endgerät betrieben werden und somit private und geschäftliche Dateien voneinander abzugrenzen.

VPP Token

Hier können Sie Ihren erworbenen VPP Token hochladen, indem Sie auf „Click here to select a file“.

Vergessen Sie anschließend nicht mit „Save“ das ganze abzuspeichern.



Knox Key

Hier können Sie Ihren erhaltenen Samsung KNOX-Key einspielen.

KNOX License Key	Hier den KNOX-Key eingeben.
------------------	-----------------------------

VPP Licenses

Sofern Sie einen VPP-Account definiert haben, erhalten Sie auf dieser Seite einen Überblick über Ihre erworbenen VPP-Apps

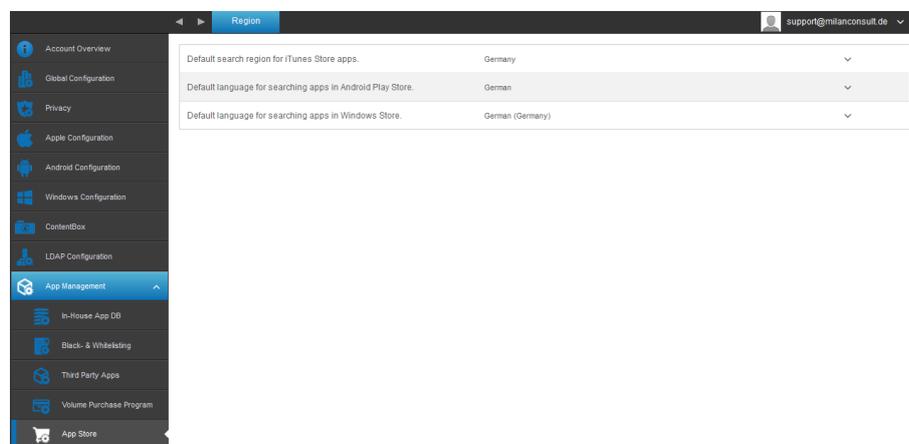
App Name	Version	Price	Assign Status	Total	Free
 Evernote	6.0.15	free	Assigned	100	100
 GoodReader for Good	4.8.0	free	Assigned	1	1

App Name	Name der App
Version	Aktuelle Version der App
Price	Ursprünglicher Preis der App
Assign Status	Zuweisungsstatus der App
Total	Gesamtanzahl an Apps
Free	Noch frei verfügbare Apps

App Store

Region

Default search region for iTunes Store apps.	Festlegung darüber, welcher iTunes Store (Apple Apps) als Standard bei der Suche benutzt werden soll.
Default language for searching apps in Android Play Store.	Festlegung darüber, welcher Google PlayStore (Android Apps) als Standard benutzt werden soll.
Default language for searching apps in Windows Store.	Festlegung darüber, welcher Windows Phone Store (Windows Phone Apps) als Standard benutzt werden soll.

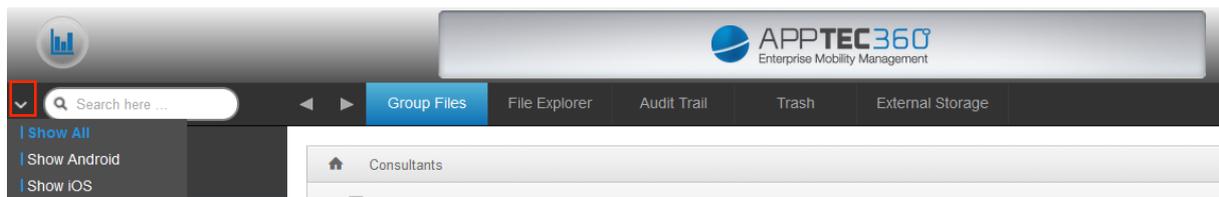


IV. Mobile Management

Oberfläche im Mobile Management

Gerätefilter

Über einen Klick auf den Pfeil links oben auf der Oberfläche können Sie diverse Filter für die Anzeige der Geräte auffinden.



Suchfenster

Das Suchfenster erlaubt es Ihnen, alle Geräte beziehungsweise Benutzer nach einem spezifischen Begriff zu durchsuchen.



Optionszahnrad

Nach einem Klick auf das entsprechende Symbol wird Ihnen eine Auflistung der zu Verfügung stehenden Optionen angezeigt. Diese ändern sich je nach aktuellem Fenster und werden in den entsprechenden Kapiteln näher erläutert.



Navigationspfeile

Mit einem Klick auf den linken Pfeil gelangen Sie auf die vorangegangene Seite, danach gelangen Sie mit einem Klick auf den rechten Pfeil auf die gerade eben verlassene Seite.



Administrationskonto-Einstellungen



My Profile	Bearbeiten Sie die Daten des Admin Kontos
Log Out	Melden Sie sich sicher von der Appliance ab

User Information

Username	Benutzername bzw. E-Mail Adresse des Kontos
Name	Vorname des Administrators
Surname	Nachname des Administrators
Login Name	Loginname des Administrators
eMail Adress	E-Mail Adresses des Administrators
Alternative eMail Adress	Alternative E-Mail Adresse des Administrators
Picture	Profilbild
Phone Number	Telefonnummer des Administrators
Mobile Number	Handynummer des Administrators
Phone Extension	Durchwahl
Location	Standort
Position	Position im Unternehmen
Usergroup	Wählen Sie aus, welcher Usergruppe Sie das Admin-Konto zuordnen wollen
Comment	Fügen Sie einen Kommentar hinzu
Enter new password	Geben Sie zur Passwortänderung das neue Passwort
Repeat new password	Wiederholen Sie das neue Passwort zur Bestätigung

Firmenverwaltung (Root-Verzeichnis) im Mobile Management



Wenn Sie sich im Root-Verzeichnis befinden (erste Gruppe) können Sie diverse Einstellung für Ihr Unternehmen in Hinsicht auf das Mobile Management durchführen.

Create a Subgroup	Untergruppe erstellen
Rename Root Node	Umbenennen des Root-Verzeichnisses (z.B. Ihr Firmenname)
Mass Enrollment	Mehrere Geräte / User auf einmal enrollen
Mass Assignment	Profile für die jeweiligen Gruppen auf einen Blick zuweisen

Create a Subgroup

Mit Create a Subgroup können Sie eine weitere Untergruppe erstellen. Sie können festlegen unter welcher Gruppe sich die Untergruppe einreihen soll. (Standardmäßig wird hier eine neue, dem Root-Verzeichnis untergeordnete, Gruppe

Create Group
✕

Group Name	<input style="width: 90%;" type="text" value="AppTec Test"/>
Parent Group	Root Node ▼

Create group

erstellt)

Rename Root Node

An dieser Stelle können Sie Ihr Root-Verzeichnis umbenennen, häufig wird hier der Firmenname eingetragen.

Default Title
✕

Root Node Name

Update Name

Mass Enrollment

Mit „Mass Enrollment“ können Sie auf einmal mehrere Geräte und User entrollen.

Mass Enrollment
✕

	Name	eMail	Alternative eMail	Phone Number	eMail	alt. eMail	SMS	iOS	Android	Windows	Phone	Tablet	Emp.	Corp.
☰	Consultants													
<input type="checkbox"/>	Lukas	██████████	██████████		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	Matthias	██████████	██████████		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	Felix	██████████	██████████		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	Fabian Kofa	██████████	██████████	██████████	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	Max Mustermann	██████████			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	Daniel	██████████	██████████		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
☰	Admins													
<input type="checkbox"/>	Tanja	██████████			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	Michael	██████████		██████████	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	Martina	██████████			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	Milan	██████████		██████████	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	Yasemin	██████████			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>					

Start Mass Enrollment
Export as CSV
Import CSV

On average it takes 10 seconds for creating and enrolling one device
 You can easily create users by adding them at the end of a exported CSV. Import the CSV afterwards and start the Mass Enrollment.
 Example: Philipp Reiss; philipp.reis@apptec360.com; pr@apptec360.com; +41 61 511 3210;.....
 Your account is limited to 25 devices. You can add 10 devices.

Sie können direkt auswählen, in welcher Form der User das Enrollment erhalten soll (eMail; alternative eMail; SMS)

Je nachdem was der User für ein Gerät erhalten soll (iOS, Android, Windows Phone) können Sie dies direkt markieren.

Die Zuweisung ob es sich um ein Smartphone oder Tablet handelt kann ebenfalls direkt eingestellt werden, je nachdem müssen Sie hier die richtige Markierung mit einem Haken setzen.

Zuletzt können Sie bestimmen, ob es sich bei dem jeweiligen Gerät um ein Firmen- oder Privatgerät (BYOD) handelt.

Sie können mit „Export as CSV“ die Informationen als CSV Tabelle exportieren, im Umkehrschluss können Sie mit „Import CSV“ auch eine CSV Datei importieren, diese sollte wie im folgenden Beispiel aussehen:

Philipp Reiss; philipp.reis@apptec360.com; pr@apptec360.com; +41 61 511 3210;;;;;

Mass Assignment

Unter „Mass Assignment“ können Sie allen Gruppen ein Profil zuweisen, dies ist unterteilt in iOS – Android – Windows

Profile Assignment
✕

Select Assignment Type iOS Android Windows

	Name	iPhone Corp.	iPhone Empl.	iPad Corp.	iPad Empl.
<input type="checkbox"/>	Consultants	Default iOS Phone Profile	Default iOS Phone Profile	Empty Profile	Profile US
<input type="checkbox"/>	Admins	Default iOS Phone Profile	Default iOS Phone Profile	iOS Tablet Admin	Empty Profile

Assign Groups

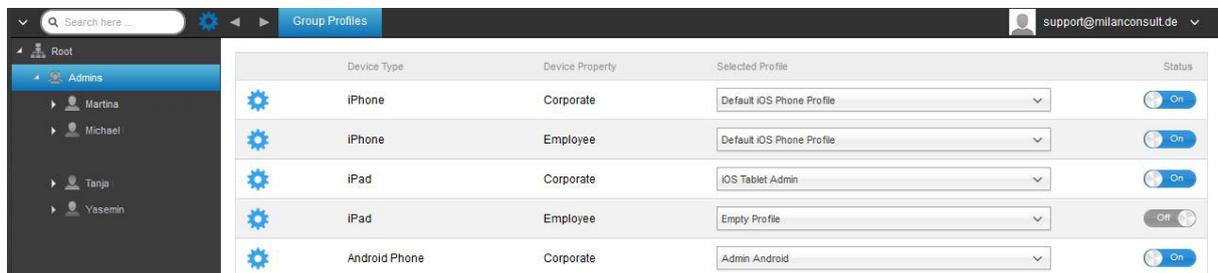
Gruppenverwaltung im Mobile Management

Ein Klick auf diese Gruppe zeigt eine Übersicht der verschiedenen Konfigurationsprofile für die entsprechenden Plattformen.

Ein Profil beinhaltet alle Einstellungsmöglichkeiten, die mit AppTec360 im Vorherein am Endgerät festgelegt werden können. Für jede Plattform können Profile für Firmengeräte (Corporate) oder Bring-Your-Own-Device Geräte (Employee) kreiert werden.

Um differenzierte Konfigurationen für Gerätegruppen, z.B. nach Standort oder Funktion, ermöglichen zu können, ist die Erstellung mehrerer Untergruppen empfohlen.

Beachten Sie die Profilverwaltung im Mobile Management



Mit diesem Zahnradmenü können Sie diverse Einstellung für die jeweilige (Unter)gruppe vornehmen.

Create a Subgroup	Untergruppe für die jeweilige (Unter)gruppe vornehmen
Edit selected Group	Ausgewählte Gruppe editieren
Delete selected Group	Ausgewählte Gruppe löschen
Mass enrollment	Mehrere Geräte / User auf einmal für das ausgewählte Profil zu enrollen
Mass Assignment	Profile für die aktuell ausgewählte Gruppe verteilen
Create a User	User für die jeweilige (Unter)gruppe erstellen

Create a Subgroup

Create Group
✕

Group Name		
Parent Group	Admins	▼

Create group

Mit Create a Subgroup können Sie eine weitere Untergruppe erstellen. Sie können festlegen unter welcher Gruppe sich die Untergruppe einreihen soll (standardmäßig gliedert sich die Untergruppe unter der aktuell ausgewählten Gruppe ein).

Edit selected Group

Hier können Sie das Profil editieren – folgende Einstellungen sind hier möglich:

- Gruppenname kann geändert werden
- Übergeordnete Gruppe kann geändert werden

Update Group
✕

Group Name	Admins	
Parent Group	Root Node	▼

Update group

Delete selected Group

Unter „delete selected Group“ werden Ihnen alle User und Geräte in der jeweilig befinden Gruppe aufgelistet, Sie sind hier in der Lage diese zu löschen.

Für einen User können Sie folgende Löschbefehle durchführen:

Delete User	User wird gelöscht
Move User To Group:	Sie können den User in eine andere Gruppe (folgende Spalte, z.B. „Admins) verschieben

Für ein Gerät können Sie folgende Löschbefehle durchführen:

Wipe & Delete	Gerät zurücksetzen und löschen
Delete from System	Gerät nur aus AppTec entfernen

[Verweis: Mass Enrollment](#)

[Verweis: Mass Assignment](#)

Create a User

Mit „Create a User“ können Sie einen neuen User hinzufügen.

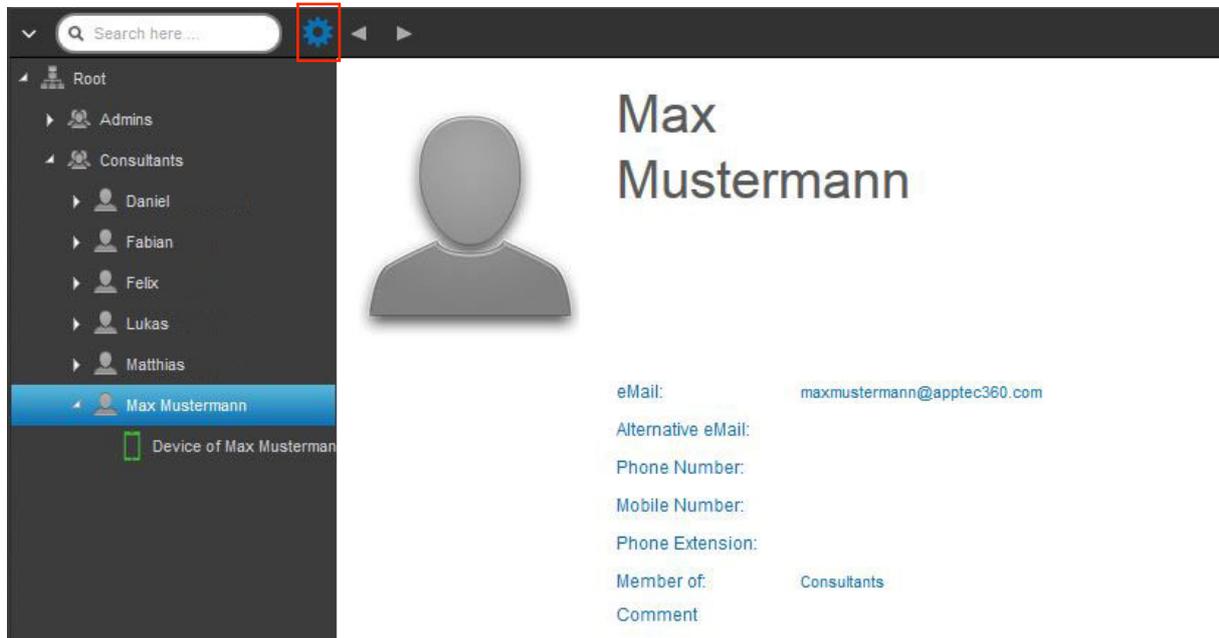
Create User
✕

Name	Pflichtfeld	Vorname des Users
Surname	Pflichtfeld	Nachname des Users
Login Name		Login Name des Users ?
eMail Address	Pflichtfeld	E-Mail Adresse des Users
Alternative eMail Address		Alternative E-Mail Adresse (des Users)
Picture	Click here to select a file	<div style="border: 1px solid blue; padding: 2px; display: inline-block;">Profilbild des Users</div> ?
Phone Number		Telefonnummer (wichtig bei SMS Enrollment)
Mobile Number		Telefonnummer
Phone Extension		Durchwahl
Location		Standort
Position		Position
Usergroup	Admins	<div style="border: 1px solid blue; padding: 2px; display: inline-block;">Zugewiesene Gruppe</div> ▼
Comment	Hier können Sie einen Kommentar hinzufügen!	

Create User

Benutzerverwaltung im Mobile Management

Wenn Sie einen bestimmten User auswählen, erhalten Sie folgende Übersicht:



Sie erhalten einen Überblick über alle Informationen die Sie zuvor bei „Create a User“ eingetragen haben.

Sie können mit dem obig angebrachten Zahnrad folgende Einstellungen vornehmen:

Edit User	User-Informationen bearbeiten
Delete user	User löschen → Delete from System = Das Gerät wird aus AppTec entfernt → Wipe & Delete = Das Gerät wird auf die Werkeinstellungen zurückgesetzt und aus AppTec entfernt
Add and enroll a Device	Ein Gerät für den ausgewählten User enrollen

Add and enroll a Device

Hier können Sie für den ausgewählten User ein Gerät enrollen, folgende Übersicht sollten Sie erhalten:

Add Device
✕

Selected User	Max Mustermann
Device name	Device of Max Mustermann
Phone Number, e.g. +49160123456	
Alternative eMail	
Device Owner	<input checked="" type="radio"/> Corporate Property <input type="radio"/> Employee Property
Choose operating system	<input checked="" type="radio"/> Android <input type="radio"/> iOS <input type="radio"/> Windows
Choose device type	<input checked="" type="radio"/> Phone <input type="radio"/> Tablet
Send enroll request now ?	<input checked="" type="checkbox"/> On ?
Send request to alternative eMail ?	<input type="checkbox"/> Off ?
Send enrollment SMS ?	<input type="checkbox"/> Off ?
You have 10 SMS credits left	

Add Device

Je nachdem was Sie für ein Gerät enrollen möchten, müssen Sie folgende Einstellungen vornehmen:

Selected User	Ausgewählter User (wird automatisch befüllt)
Device Name	Wird automatisch ausgefüllt (Device of „Name des Users“) – kann jedoch abgeändert werden
Phone Number	Telefonnummer, wird automatisch befüllt (sofern beim User angegeben) – kann jedoch hier hinzugefügt oder abgeändert werden
Alternative eMail	Alternative E-Mail Adresse, wird automatisch befüllt (sofern beim User angegeben) – kann jedoch hier

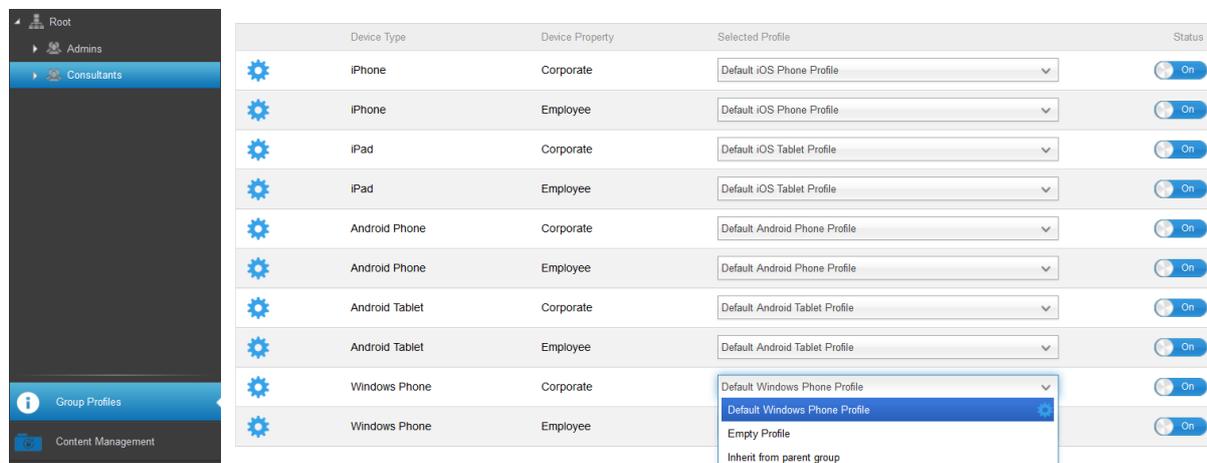
	hinzugefügt oder abgeändert werden
Device Owner	Corporate Property = Firmengerät Employee Property = BYOD Geröt
Choe operation System	Sie können hier zwischen Android, iOS und Windows Phone Geräte wählen
Send enroll request?	Die E-Mail wird sofort an die angegebene Haupt E-Mail Adresse verschickt und der User wird aufgefordert sein Gerät einzubinden
Send request to alternative eMail?	Die enroll E-Mail zusätzlich oder ausschließlich (falls „Send enroll request?“ deaktiviert wurde) an die alternative E-Mail Adresse zu verschicken (E-Mail unterscheidet sich nicht im Gegensatz zur „normalen“ enroll Request E-Mail)
Send enrollment SMS?	Ein enrollment request über SMS zu verschicken (die „Phone Number“ muss eingetragen sein)

Nachdem der Enrollment Request verschickt wurde, wir bereits ein Gerät (rot markiert) angezeigt.

Sobald das Gerät erfolgreich eingebunden ist, wird das Gerät nach kurzer Zeit grün markiert und ist somit bereit diverse Restriktionen, Apps, etc. zu erhalten.

Profilverwaltung im Mobile Management

Nach einem Klick auf eine Gruppe erhalten Sie eine Übersicht aller zu konfigurierenden Geräteplattformen und der entsprechend zugewiesenen Profile.



	Nehmen Sie Einstellungen für das gerade ausgewählte Profil vor
Device Type	Gerätetyp bzw. Modell
Device Property	Eigentümer des Gerätes (Corporate = Firmeneigentum, Employee = Privatgerät d. Mitarbeiters)
Selected Profile	Ausgewähltes Profil (Das Zahnrad öffnet den Konfigurationsdialog des Profils)
Status	On/Off (Das Profil ist aktiviert/deaktiviert)

Wenn Sie das Zahnrad anwählen, erhalten Sie folgende Optionen:

Create a profile

Für jeden Eintrag bzw. Plattform können Sie ein neues Profil anlegen und konfigurieren. Nachdem Sie diesen Unterpunkt angeklickt haben, wird das Profil direkt erstellt und Sie können direkt mit der Konfiguration von iOS, Android und Windows Phone beginnen.

Edit Profile

Nach einem Klick auf „Edit Profile“ gelangen Sie direkt in die Konfigurationsoberfläche für das entsprechende Profil und können die Einstellungen anpassen.

Copy Profile

Mit Hilfe der „Copy Profile“ Funktion können Sie die Anpassungen/Einstellungen eines bereits vorhandenen Profils kopieren und in ein neues Profil einfügen.

Copy Group Profile
✕

Source Profile Name	Default iOS Phone Profile
New Profile Name	Copy of Default iOS Phone Profile
Profile Type	Phone Profile ▼

Copy

Source Profile Name	Name des zu kopierenden Profils
New Profile Name	Name des neuen Profils
Profile Type	Typ des Profils (Phone/Tablet)

Wenn Sie nun auf „Copy“ drücken, wird das Profil erstellt und kann nun der Gruppe zugewiesen werden

Delete Profile

Hier können Sie ein Profil endgültig löschen. Beachten Sie, dass bei der Löschung und nachfolgendem „Assign Now“ des Profils die Konfiguration entsprechend auf den Endgeräten der betroffenen Gruppe verschwindet und nicht wiedergestellt werden kann!

Delete Group Profile
✕

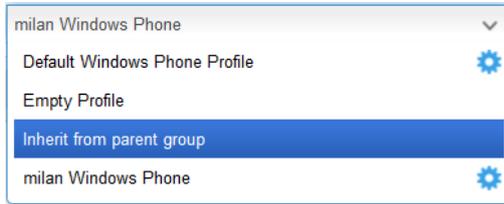
Profile to Delete	Default iOS Phone Profile
-------------------	---------------------------

Cancel

Delete

Vererbung von Profilen

Bei der Auswahl der Profile steht auch die Option „Inherit from parent group“ zur Verfügung.



Wenn dieses Profil aktiviert ist, dann wird für den entsprechend ausgewählten Gerätetyp das Profil der übergeordneten Gruppe (und jeweiligem Gerätetyp) verwendet. Beachten Sie also, dass Änderungen an diesem Profile durchaus mehrere Gruppen betreffen können.

Diese Einstellung ist auch als Standardwert eingestellt, wenn eine neue Untergruppe erstellt wird.

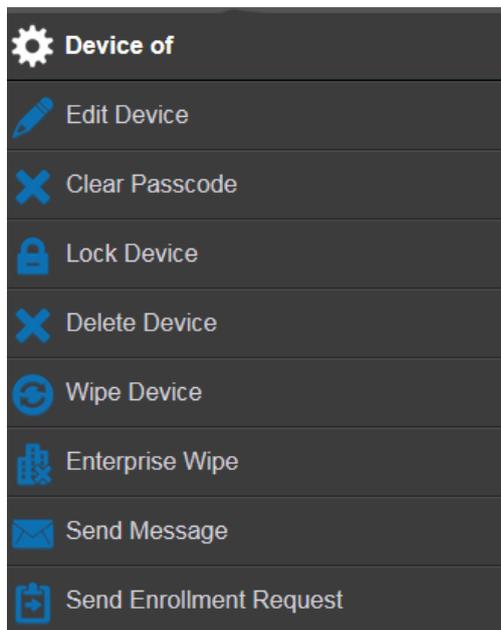
Ebenso ist die Einstellung „Empty Profile“ vorhanden, welche einem leeren Profil entspricht, d.h. im Endeffekt werden keine Einstellungen am Endgerät vorgenommen.

Geräteverwaltung im Mobile Management

Wenn Sie ein Gerät auswählen, können Sie über das „Zahnrad“ diverse Aktionen ausführen.

Diese unterscheiden sich je nach Betriebsplattform (Android, iOS, Windows Phone)

Android



Edit Device	Geräte Informationen ändern
Clear Passcode	Passcode des Gerätes löschen
Lock Device	Gerät sperren (Sperrbildschirm)
Delete Device	Gerät aus AppTec entfernen
Wipe Device	Geräte auf die Werkseinstellungen zurücksetzen
Enterprise Wipe	Von AppTec zur Verfügung gestellte Informationen, Apps, Profile werden gelöscht (Gerät wird vom MDM getrennt)
Send Message	Push Benachrichtigung an das Gerät versenden Nachricht wird in der AppTec App angezeigt (Message Tab)
Send Enrollment Request	(erneuten) Enrollment request versenden

Edit Device

Hier können Sie diverse Informationen des Geräts anpassen.

Update Device
✕

Selected User	Matthias
Device name	Device of Matthias
Phone Number, e.g. +49160123456	
Device Owner	<input checked="" type="radio"/> Corporate Property <input type="radio"/> Employee Property
Choose device type	<input checked="" type="radio"/> Phone <input type="radio"/> Tablet

Save

Selected User	Benutzer des Gerätes
Device name	Name des Gerätes
Phone Number	Telefonnummer des Gerätes
Device Owner	Corporate = Firmeneigentum Employee = Mitarbeitereigentum
Choose device typ	Typ des ausgewählten Gerätes

Clear Passcode

Hier können Sie das Gerätepasswort des ausgewählten Gerätes entfernen. Bei Android wird der Passcode standardmäßig auf „1234“ gesetzt – dieses kann und sollte der User nachträglich wieder abändern.

Lock Device

Hier wird lediglich einen Sperrbefehl an das Endgerät verschickt (Sperrbildschirm).

Delete Device

Hier kann ein Löschbefehl durchgeführt werden, Sie können erneut unterscheiden, ob das Gerät nur aus AppTec („Delete from System“) entfernt werden soll oder ob das Gerät aus AppTec entfernt werden soll und zusätzlich sich auf die Werkseinstellungen zurücksetzen soll („Wipe & Delete“).

Delete Device
✕

Are you sure to delete this device ?

Device:	Device of Matthias	Delete from System ▼	Root Node ▼
---------	--------------------	----------------------	-------------

Process Delete

Wipe Device

Unter „Wipe Device“ können Sie einen vollständigen Wipe des Gerätes durchführen, das Gerät wird dann auf die Werkseinstellungen zurückgesetzt.

Zusätzlich können Sie, falls sich im Gerät eine SD Karte befindet, die SD Karte löschen, dies können Sie tun indem Sie „Wipe SD Card too?“ auf „On“ setzen.



Wipe Device ✕

Are you sure to wipe the device ?

Wipe SD Card too ? Off

No
Yes

Enterprise Wipe

Dies ist der empfohlene Weg um eine Trennung zum MDM durchzuführen.

Nur von AppTec zur Verfügung gestellte Informationen, Apps, Profile werden gelöscht, somit werden alle Firmendaten auf dem Endgerät nicht mehr zur Verfügung stehen, der private Bereich ist jedoch nicht betroffen und bleibt weiterhin auf dem



Enterprise Wipe device? ✕

Are you sure to Enterprise Wipe the device ?

No
Yes

Endgerät bestehen.

Send Message

Send a message
✕

Subject	Wichtig! Bitte bei Ihrer IT melden!
Message	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;"> Sehr geehrter Herr Mustermann, bitte melden Sie sich umgehend bei Ihrer IT-Abteilung. </div>

Send Message

Hier können Sie eine Push Benachrichtigung an das jeweilige Endgerät versenden.

Send Enrollment Request

Mit „Send Enrollment Request“ können Sie (nochmals) ein Enrollment Request an den jeweiligen User schicken.

Bitte beachten Sie, dass nur der letzte Enrollment – Request gültig ist.

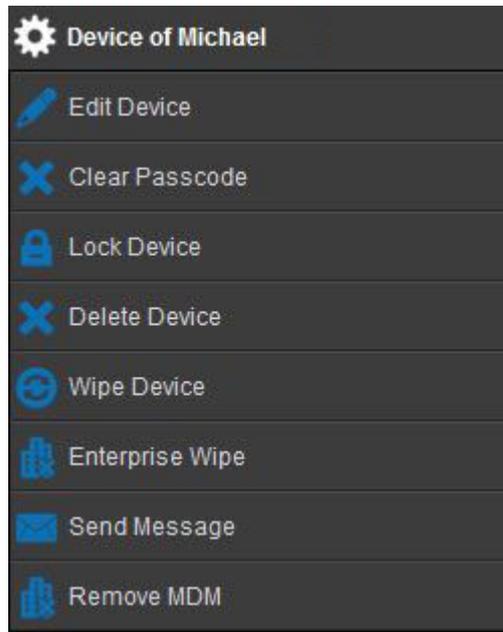
Send Enrollment Request
✕

Send enroll request now ?	<input checked="" type="checkbox"/> On	?
Alternative eMail address	matthias [redacted] .com	
Send to alt. eMail address ?	<input type="checkbox"/> Off	?
Send enroll SMS ?	<input type="checkbox"/> Off	?

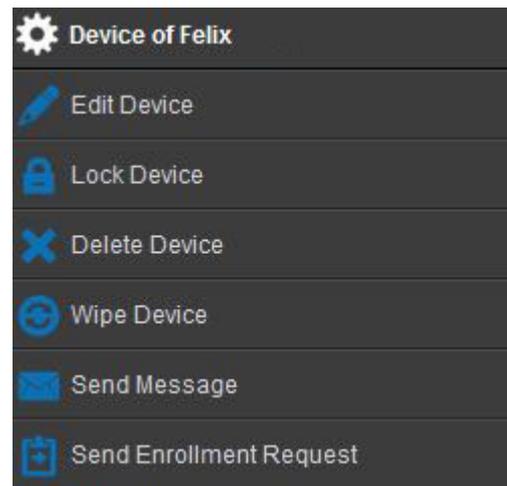
Enroll now

iOS

Wenn das Gerät eingebunden (grün) ist:



Wenn das Gerät nicht eingebunden (rot) ist:



Edit Device	Gerät editieren
Clear Passcode	Das Gerätepasswort wird gelöscht
Lock Device	Gerät sperren (Sperrbildschirm)
Delete Device	Gerät aus AppTec entfernen
Wipe Device	Geräte auf die Werkseinstellungen zurücksetzen
Enterprise Wipe	Von AppTec zur Verfügung gestellte Informationen, Apps, Profile werden gelöscht (Gerät wird vom MDM getrennt)
Send Message	Push Benachrichtigung an das Gerät versenden Nachricht wird in der AppTec App angezeigt (Message Tab)
Send Enrollment Request	(nochmaliger) Enrollment request versenden
Remove MDM	Das MDM vom Endgerät entfernen (gleicher Effekt wie der „Enterprise Wipe“)

Edit Device

Hier können Sie diverse Informationen des Geräts anpassen.

Update Device
✕

Selected User	Matthias
Device name	Device of Matthias
Phone Number, e.g. +49160123456	
Device Owner	<input checked="" type="radio"/> Corporate Property <input type="radio"/> Employee Property
Choose device type	<input checked="" type="radio"/> Phone <input type="radio"/> Tablet

Save

Clear Passcode

Unter „Clear Passcode“ können Sie das Gerätepasswort remote auf dem Endgerät entfernen, der User wird anschließend aufgefordert ein neues Passwort (je nach Passcode Richtlinien) zu vergeben.

Clear Passcode?
✕

Are you sure to remove the passcode from the device ?

No

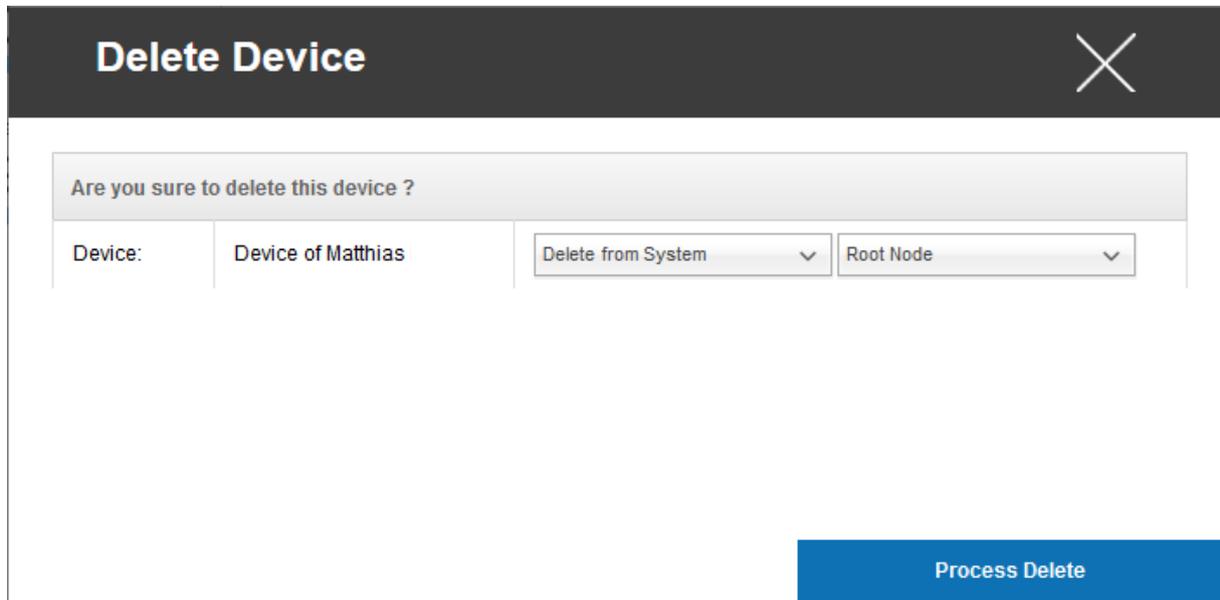
Yes

Lock Device

Hier wird lediglich einen Sperrbefehl an das Endgerät verschickt (Sperrbildschirm).

Delete Device

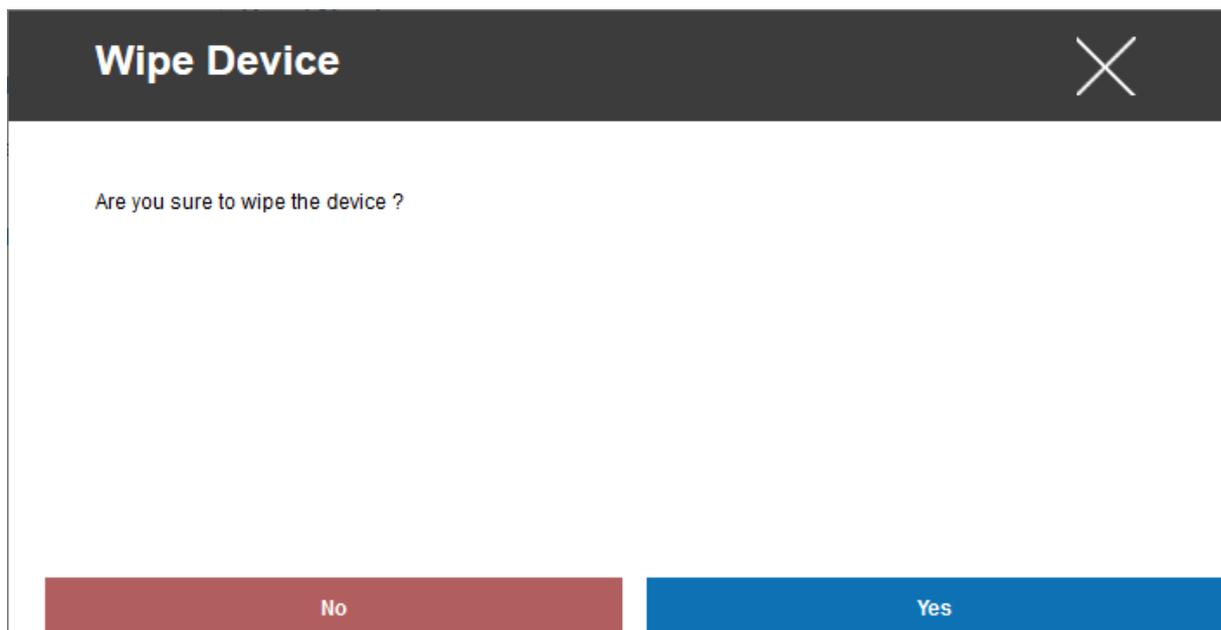
Hier kann ein Löschbefehl durchgeführt werden, Sie können erneut unterscheiden, ob das Gerät nur aus AppTec („Delete from System“) entfernt werden soll oder ob das Gerät aus AppTec entfernt werden soll und zusätzlich sich auf die



Werkseinstellungen zurücksetzen soll („Wipe & Delete“).

Wipe Device

Unter „Wipe Device“ können Sie einen vollständigen Wipe des Gerätes durchführen, das Gerät wird dann auf die Werkseinstellungen zurückgesetzt.



Enterprise Wipe

Nur von AppTec zur Verfügung gestellte Informationen, Apps, Profile werden gelöscht, somit werden alle Firmendaten auf dem Endgerät nicht mehr zur Verfügung stehen, der private Bereich ist jedoch nicht betroffen und bleibt weiterhin auf dem



Endgerät bestehen.

Send Message

Hier können Sie eine Push Benachrichtigung an das jeweilige Endgerät versenden.

Send a message ✕

Subject	Wichtig! Bitte bei Ihrer IT melden!
Message	<div style="border: 1px solid #ccc; padding: 5px;"> Sehr geehrter Herr Mustermann, bitte melden Sie sich umgehend bei Ihrer IT-Abteilung. </div>

Send Message

Send Enrollment Request

Mit „Send Enrollment Request“ können Sie (nochmals) ein Enrollment Request an den jeweiligen User schicken.

Send Enrollment Request ✕

Send enroll request now ?	<input checked="" type="checkbox"/> On	?
Alternative eMail address	matthias <input type="text"/> com	
Send to alt. eMail address ?	<input type="checkbox"/> Off	?
Send enroll SMS ?	<input type="checkbox"/> Off	?

Enroll now

Remove MDM

Mit „Remove MDM“ können Sie das MDM Profil und alles weitere von AppTec zur Verfügung gestellte auf dem Endgerät entfernen.
Dieser Befehl führt dieselbe Aktion wie der „Enterprise Wipe“ durch.

Remove MDM from device?

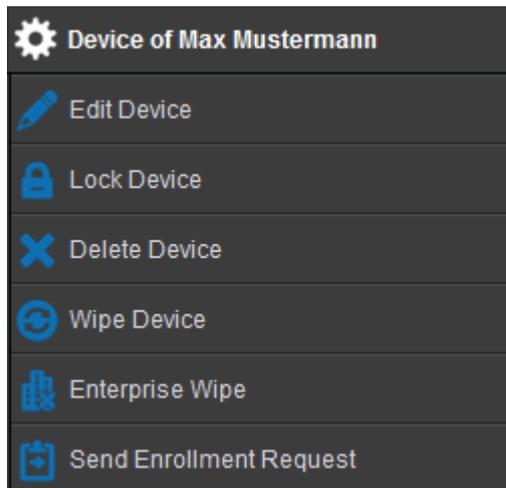


Are you sure to remove MDM from device ?

No

Yes

Windows



Edit Device	Gerät editieren
Lock Device	Gerät sperren (Sperrbildschirm)
Delete Device	Gerät aus AppTec entfernen
Wipe Device	Geräte auf die Werkseinstellungen zurücksetzen
Enterprise Wipe	Von AppTec zur Verfügung gestellte Informationen, Apps, Profile werden gelöscht
Send Enrollment Request	(nochmaliger) Enrollment request versenden

Edit Device

Hier können Sie diverse Informationen des Geräts anpassen.

Update Device
✕

Selected User	Matthias
Device name	Device of Matthias
Phone Number, e.g. +49160123456	
Device Owner	<input checked="" type="radio"/> Corporate Property <input type="radio"/> Employee Property
Choose device type	<input checked="" type="radio"/> Phone <input type="radio"/> Tablet

Save

Lock Device

Hier wird lediglich einen Sperrbefehl an das Endgerät verschickt (Sperrbildschirm).

Delete Device

Hier kann ein Löschbefehl durchgeführt werden, Sie könne erneut unterscheiden, ob das Gerät nur aus AppTec („Delete from System“) entfernt werden soll oder ob das Gerät aus AppTec entfernt werden soll und zusätzlich sich auf die

Delete Device
✕

Are you sure to delete this device ?

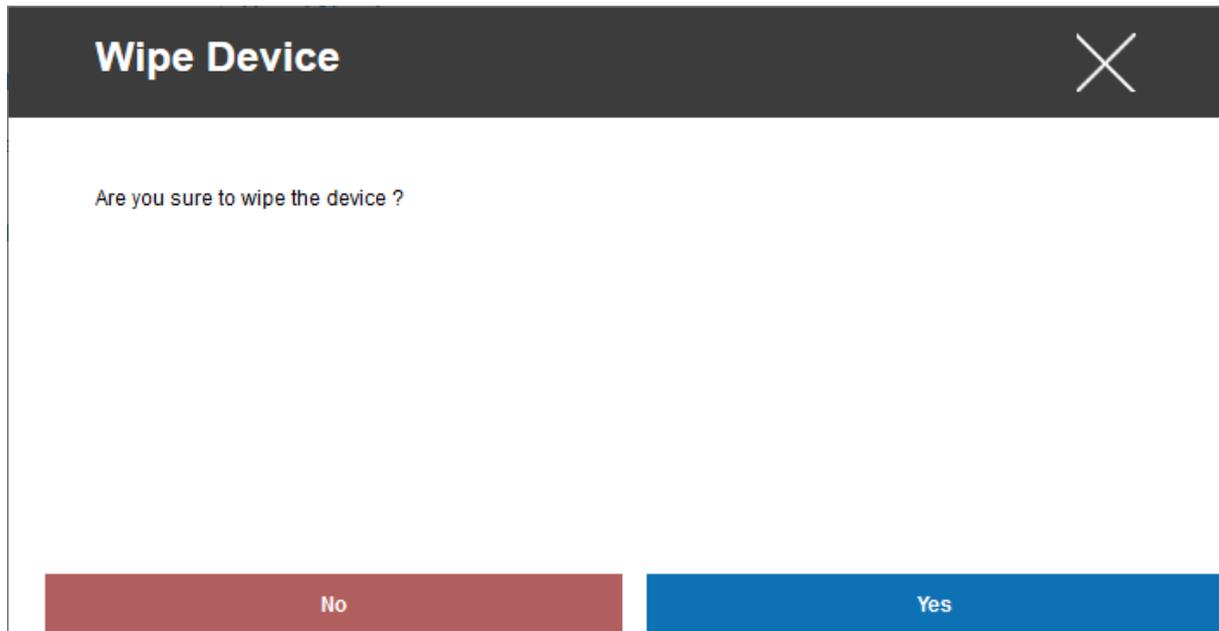
Device:	Device of Matthias	Delete from System ▼	Root Node ▼
---------	--------------------	----------------------	-------------

Process Delete

Werkseinstellungen zurücksetzen soll („Wipe & Delete“).

Wipe Device

Unter „Wipe Device“ können Sie einen vollständigen Wipe des Gerätes durchführen, das Gerät wird dann auf die Werkseinstellungen zurückgesetzt.



Enterprise Wipe

Nur von AppTec zur Verfügung gestellte Informationen, Apps, Profile werden gelöscht, somit werden alle Firmendaten auf dem Endgerät nicht mehr zur Verfügung stehen, der private Bereich ist jedoch nicht betroffen und bleibt weiterhin auf dem



Endgerät bestehen.

Send Enrollment Request

Mit „Send Enrollment Request“ können Sie (nochmals) ein Enrollment Request an den jeweiligen User schicken.

Send Enrollment Request
✕

Send enroll request now ?	<input checked="" type="checkbox"/> On	?
Alternative eMail address	matthias <input type="text"/> com	
Send to alt. eMail address ?	<input type="checkbox"/> Off	?
Send enroll SMS ?	<input type="checkbox"/> Off	?

Enroll now

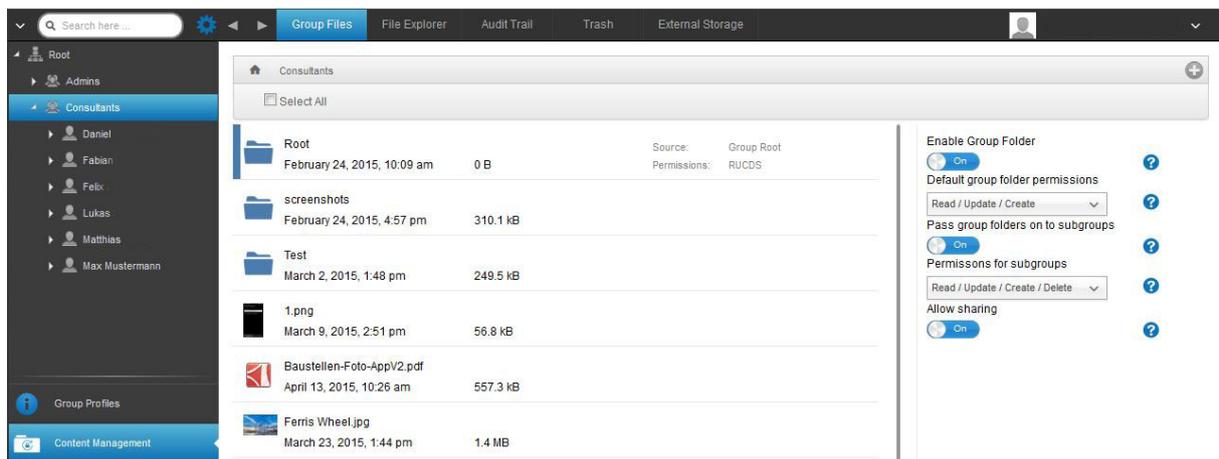
Content Management

Wenn Sie sich auf einer Gruppe befinden, können Sie mit dem „Content Management“ die ContentBox von AppTec verwalten.

Mit der Content Box können Sie Dokumente und andere Firmendaten sicher auf die Endgeräte verteilen.

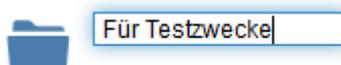
Group Files

„Group Files“ stellt den zentralen Baustein der ContentBox dar, hier können Sie allerlei Einstellungen vornehmen, Ihre Dokumente hochladen, neue Ordner anlegen, etc.



Mit dem  Symbol oben rechts können Sie über „Add Folder“ einen neuen Ordner anlegen, der der jeweiligen Gruppe zugeordnet werden soll.

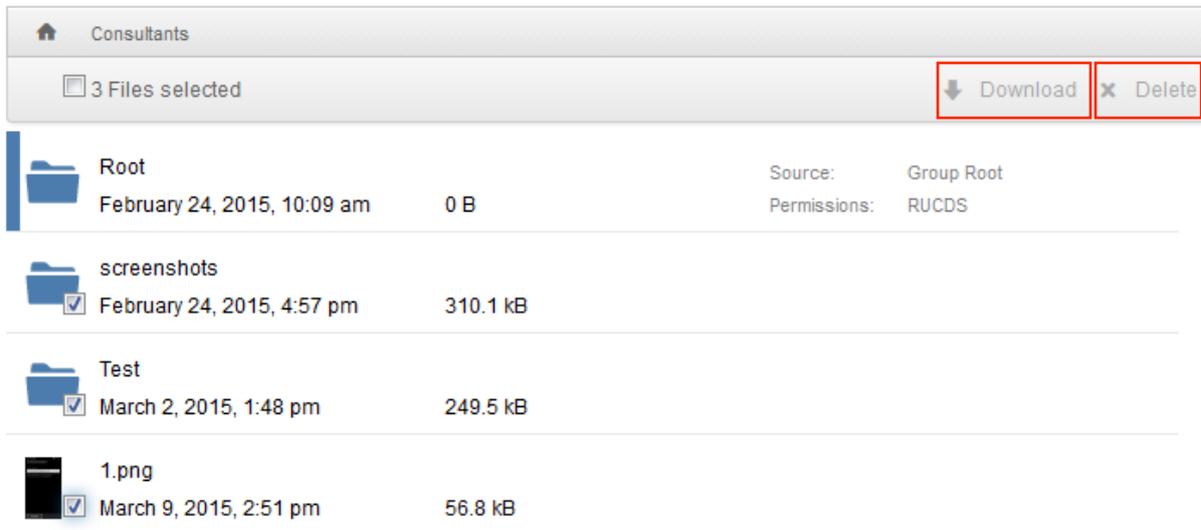
Sie können den Ordner beliebig benennen.



Über „Upload Files“ können Sie eine neue Datei hochladen, Ihr Standard-Explorer wird hier geöffnet. Selbstverständlich können Sie diese zwei Aktionen in jedem (Unter)Ordner durchführen.

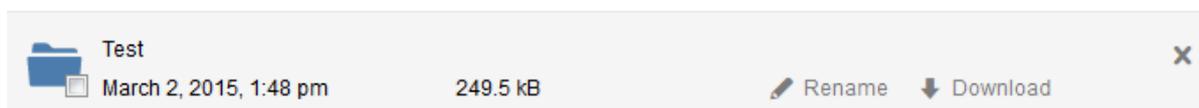
Mit dem  Symbol oben links kommen Sie immer wieder zurück ins Hauptverzeichnis.

Sie können mehrere Ordner und Dateien auswählen und sich diese per „Download“ herunterladen oder Sie löschen diese indem Sie „Delete“ anklicken.



Ebenfalls können Sie mit **Select All** alle Dateien und Ordner auswählen und die Befehle „Download“ und „Delete“ ausführen.

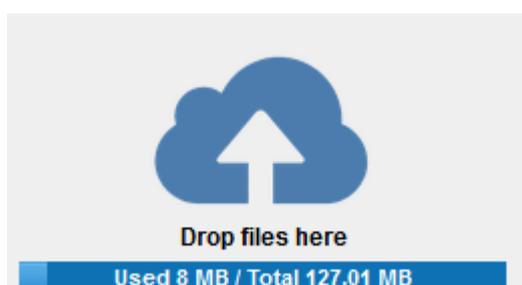
Wenn Sie den Mauszeiger über ein Ordner oder über einer Datei bewegen, erscheint Ihnen folgende Ansicht:



- Mit „Rename“ können Sie den Ordner / die Datei umbenennen
- Mit „Download“ können Sie sich den Ordner / die Datei herunterladen
- Mit dem „x“ können Sie den Ordner / die Datei löschen

Enable Group Folder	Falls aktiviert, alle Mitglieder in dieser Gruppe haben Zugriff auf den jeweiligen Ordner
Default group folder permissions	Berechtigung für die User in der ausgewählten Gruppe Read = nur Leseberechtigung Update = Update-Berechtigung Create = Erstell-Berechtigung Delete = Löschberechtigung
Pass group folders on to subgroups	Falls aktiviert, können die dementsprechenden Untergruppen auf die Dateien der übergeordnete Gruppe zugreifen
Permissions for subgroups	Berechtigung für die jeweilige Untergruppe Read = nur Leseberechtigung Update = Update-Berechtigung Create = Erstell-Berechtigung Delete = Löschberechtigung
Allow Sharing	Falls aktiviert, kann der User Dateien per Link teilen

Um Dateien hochzuladen, können Sie auch dieses Feld benutzen, indem Sie einfach per Drag & Drop eine Datei auf dieses Fenster ziehen, ebenfalls können Sie auf dieses Feld klicken, um mit Hilfe des Explorers eine Datei auszuwählen und hochzuladen.



File Explorer

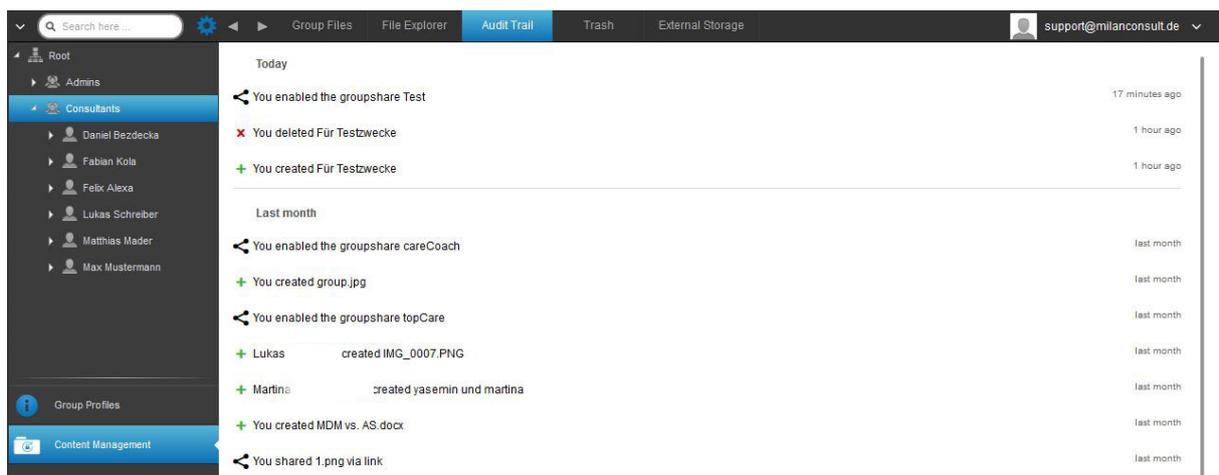
Mit dem „File Explorer“ können Sie alle Ordner und Dateien – unabhängig in welcher Gruppe Sie sich befinden – verwalten.

Sie finden die bereits schon beim „Group Files“ gelernten Einstellungen und Knöpfe hier ebenfalls wieder.



Audit Trail

Im „Audit Trail“ können Sie eine Historie einsehen, welcher User etwas erstellt, gelöscht oder geteilt hat, somit können Sie zu jeder Zeit nachvollziehen was mit den Firmendaten gemacht wurde.



Trash

Sollten Sie (ausversehen) etwas gelöscht haben, können Sie diese Ordner und Dateien unter „Trash“ einsehen und bei Belieben wieder herstellen.

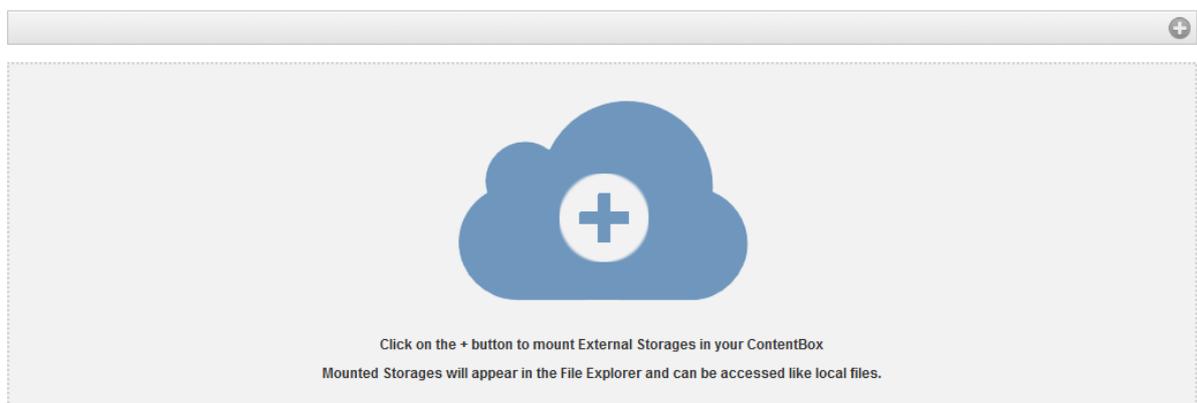
- Mit „Undelete“ können Sie die Datei / den Ordner wiederherstellen.
- Mit „Delete“ können Sie die Datei / den Ordner endgültig löschen – Sie müssen den Löschvorgang nochmals bestätigen.

Bitte beachten Sie dass der sich im Papierkorb befindende belegte Speicherplatz vom „Total Space“ abgezogen wird – dies ist seitens ownCloud bedingt.



External Storage

Unter dem Punkt „External Storage“ können Sie einen externen Speicher anbinden.



Mit dem  Symbol kann ein (weiterer) Speicher hinzugefügt werden.

Type	Amazon S3 FTP SFTP ownCloud WebDAV Windows Share Sharepoint
Amazon S3	
Display Name	Anzuzeigender Name
Access Key	Zugangsschlüssel
Secret Key	Sicherheitsschlüssel

Bucket	Eindeutige Identität des Unterordners der Ihnen zugewiesen ist
Hostname (optional)	Hostname (optional)
Port (optional)	Port (optional)
Region	Region (optional)
Enable SSL	Aktivierung von SSL
Enable Path Style	Eindeutige Path Adresse die Ihnen zugewiesen ist
FTP	
Display Name	Anzuzeigender Name
Host	Host-Adresse
Username	Benutzername
Password	Passwort
Root	Hauptverzeichnis
Secure ftps://	
SFTP	
Display Name	Anzuzeigender Name
Host	Host-Adresse
Username	Benutzername
Password	Passwort
Root	Hauptverzeichnis
ownCloud	
Display Name	Anzuzeigender Name
URL	ownCloud URL
Username	Benutzername
Password	Passwort
Remote Subfolder	Standard Ordner
Secure https://	
WebDAV	
Display Name	Anzuzeigender Name
URL	WebDAV URL
Username	Benutzername
Password	Passwort
Root	Hauptverzeichnis
Secure https://	
Windows Share	Der Support für Windows Share wird demnächst erscheinen
Sharepoint	Der Support für Microsoft Sharepoint wird demnächst erscheinen

Konfiguration iOS

General

Je nachdem ob Sie aktuell eine Gruppe oder ein Gerät ausgewählt haben, unterscheidet sich die Darstellung und deren Unterpunkte – bitte beachten Sie dies sorgfältig!

Profile Information

Sollten Sie sich in einem Profil befinden, erhalten Sie hier einen kurzen Überblick über das Profil in Bezug auf Name, OS, Erstellungsdatum, Autor, etc.

Profile Name	Name des Profils – kann direkt hier umbenannt werden
Operating System	Für welches Betriebssystem das Profil gilt
Created At	Erstelldatum
Created By	Ersteller des Profils
Last Change	Datum und Uhrzeit an dem die letzten Änderungen vorgenommen wurden
Changed By	Anzeige darüber von wem die letzte Änderung vorgenommen wurde
Profile Revision	Anzahl wie oft das Profil bereits geändert wurde

General Information

Sollten Sie sich direkt auf einem Gerät befinden, erhalten Sie hier einen kurzen Überblick über Ihr ausgewähltes Gerät.

Device Name	Name des Geräts
Phone Number	Telefonnummer des Geräts
Model	Modellbezeichnung
Operating System	Betriebssystem
Serial Number	Seriennummer des Geräts
Device Ownership	Firmen- oder Privatgerät Corporate = Firmengerät Employee = Privatgerät
Device Type	Gerätetyp (Tablet oder Phone)
Jailbroken	Ob sich auf dem Gerät ein Jailbreak befindet
Supervised	Anzeige darüber ob es sich um ein Supervised Gerät handelt
Compliant	Ob gegen über irgendwelchen Richtlinien verstoßen wurde
Last Seen	Status wann sich das Gerät zuletzt am AppTec Server gemeldet hat

Settings

Diese Settings beinhaltet den Gerätenamen und einen vordefinierten Hintergrund.

Name device to system name	Der Name der in der AppTec Console vergeben wird (in der linken Strukturordnung), wird dann derselbe wie auf dem jeweiligen Endgerät (einsehbar in in den Geräte Einstellungen)
Use custom wallpaper (supervised devices only)	Hier können Sie einen Hintergrund vordefinieren, der auf dem Endgerät angezeigt werden soll (z.B. für eine Art Firmenbranding des Gerätes) Ist nur im Supervised Mode verfügbar!

Config Revision

Hier erhalten Sie eine Übersicht welches Gruppenprofil dem Gerät zugewiesen ist. Wenn sie auf das Gruppenprofil klicken, kommen Sie direkt zu diesem Profil und können Einstellungen vornehmen.

Mit dem  Symbol können Sie die zugewiesenen Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Mit dem  Symbol können Sie alle getätigten Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Device Log

Unter diesem Punkt erhalten Sie eine Auflistung aller Aktionen, welche in Bezug auf das Enderät stattgefunden haben, u.a. Erstellung, Löschung etc.

Event Log (last 50 events)		
	Event	Date
	User deleted MDM-Profile from device	
	Device enrolled	
	Device enrollment request sent	
	Device assigned to user	
	Device created	

Asset Management (nur auf Device Ebene)

Asset Management (nur auf Device Ebene)

Device Info

Model	Modellbezeichnung des Geräts
Operating System	Betriebssystem
OS Version	Betriebssystem Version
Serial Number	Seriennummer
UDID	UDID des Gerätes
Device Name	Gerätename
Supervised	Zeigt an, ob das Gerät supervised ist
Battery Status	Batterieanzeige

Wi-Fi

IP Address	IP Adresse des Gerätes
WiFi MAC	WiFi MAC Adresse

Cellular

Status	Status (SIM Karte vorhanden)
Phone Number	Telefonnummer
Roaming Status	Aktueller Roaming Status
Roaming (Voice/Data)	Romaing Status für Anrufe / Daten
IP Address	IP Adresse
IMEI	IMEI-Nummer
Operator/Carrier	Mobilfunk Anbieter
SIM Carrier Network	Mobilfunknetzwerk der SIM-Karte
Carrier Version	
Modem Firmware	Firmware des Modems
Current MCC/MNC	Siehe „SIM MCC/MNC“
SIM MCC/MNC	Der Mobile Country Code ist eine von der ITU im Standard E.212 festgelegte Länderkennung, die zusammen mit dem Mobile Network Code (MNC) zur Identifizierung eines Mobilfunknetzes verwendet wird (=Ländercode) Wenn man in ein anderes Mobilfunknetz geht sind deshalb der „Current MCC/MNC“ und „SIM MCC/MNC“ unterschiedlich.

Bluetooth

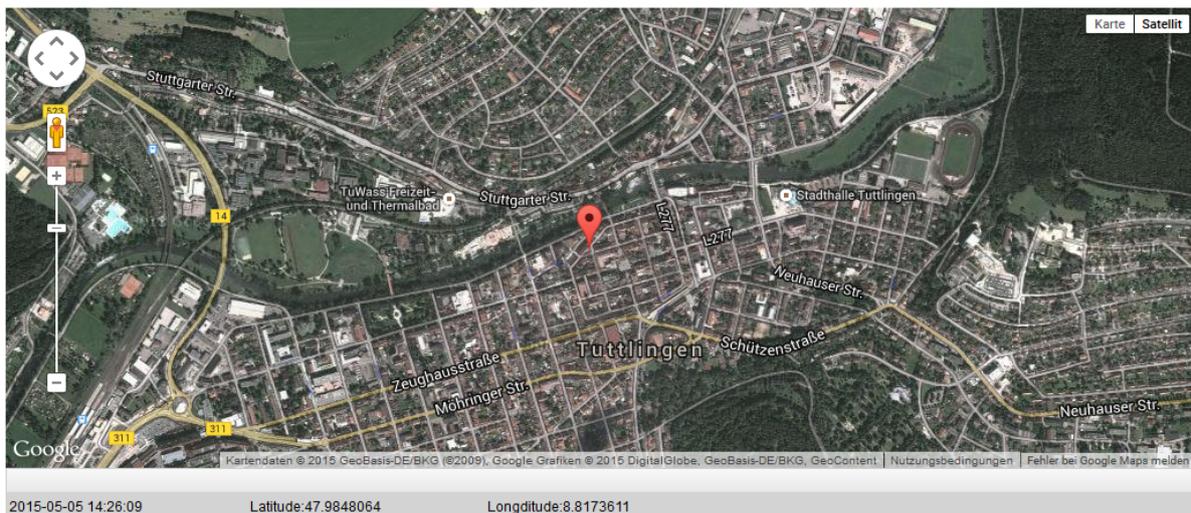
Bluetooth MAC	Bluetooth MAC Adresse
---------------	-----------------------

Security Management

Anti Theft (nur auf Device Ebene)

GPS Information (nur auf Device Ebene)

Hier können Sie den aktuellen / letzten Standort des Geräts ermitteln. Die Lokalisierung kann mit einem oder sogar zwei Passwörtern geschützt werden –
Siehe: *General Settings – Privacy – GPS Access*



Wipe & Lock (nur auf Device Ebene)

Unter „Wipe & Lock“ können Sie folgende drei Aktionen durchführen:

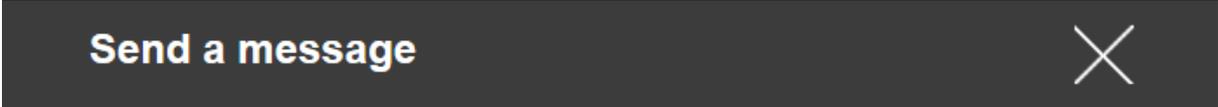
Full Wipe	Das Gerät wird auf die Werkseinstellungen zurückgesetzt (sowohl geschäftliche, als auch persönliche Daten werden gelöscht)
Enterprise Wipe	Nur die Firmendaten werden vom Endgerät entfernt (Alle Apps, Daten, etc. die von AppTec übergeben wurden)
Lock Screen	Bildschirm Sperre wird aktiviert, es ist ausreichend das Gerät mit dem Geräte-Passwort/PIN wieder zu entsperren

Message (nur auf Device Ebene)

Mit „Open Message Dialog“ können Sie eine Push-Nachricht versenden.



Anschließend sollte sich folgendes Fenster öffnen, dies können Sie mit einem Subject (Betreff) und einer Message (Nachricht) füllen und an das ausgewählte Endgerät versenden.



Subject	Test: Bitte bei Ihrer IT melden
Message	<div data-bbox="710 913 1252 1064" style="border: 1px solid #ccc; padding: 5px;"> <p>Diese Nachricht dient zur Testzwecken! Bitte melden Sie sich bei Ihrer EDV Abteilung.</p> <p>Mit freundlichen Grüßen</p> <p>Ihre IT-Abteilung</p> </div>



Security Configuration

Passcode

Legen Sie hier die Einstellungen für das Gerätepasswort fest

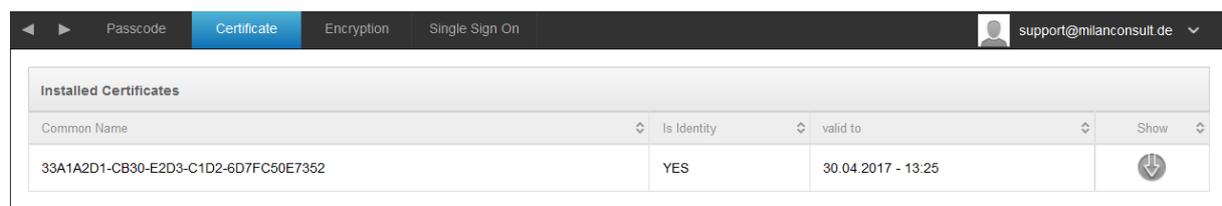
Code deactivation allowed	Wenn diese Einstellung aktiviert ist, findet keine Aufforderung für das Setzen eines Passworts statt Sobald ein Passwort gesetzt ist, kann es nicht mehr deaktiviert werden
Allow simple value	Erlaube die Benutzung gleicher aufsteigender und absteigender Zeichenketten (z.B. 1234, 1111)
Require alphanumeric value	Passwörter müssen mindestens einen Buchstaben enthalten
Minimum passcode length	Minimale Länge des Passworts
Minimum number of complex characters	Minimale Anzahl alphanumerischer Zeichen im Passwort
Maximum passcode age	Anzahl der Tage, nach welchen das Passwort geändert werden muss
Maximum Auto-Lock	Maximale Dauer, nach welcher sich das Gerät sperrt
Maximum grace period for device lock	Dauer, nach welcher das Gerät in den gesperrten Stand-By geht
Maximum number of failed attempts	Maximale Anzahl an Fehlversuchen
Maximum passcode age (1-730 days)	Maximale Passwortlebensdauer
Passcode history (1-50 passcodes)	Das Benutzen eines alten Passworts ist nach dieser Anzahl wieder erlaubt

Ein Klick auf den Papierkorb öffnet den Passwort-Reset Dialog, mit welchem ein vergessenes Gerätepasswort entfernt werden kann.

Certificate (nur auf Device Ebene)

Installed Certificates

Zeigt die auf dem Gerät verfügbaren Zertifikate an



Common Name	Is Identity	valid to	Show
33A1A2D1-CB30-E2D3-C1D2-6D7FC50E7352	YES	30.04.2017 - 13:25	

Encryption

Require storage encryption	Aktivieren Sie die eingebaute Verschlüsselungsfunktion des Gerätes
----------------------------	--

Single Sign-On

Unter dem Punkt "Single Sign-On" können Sie eine Kerberos Authentifizierung einstellen.

Hier legen Sie die Zugangsdaten und die jeweiligen URLs / Apps fest, die die Tokens des Kerberos benutzen dürfen.

Verfügbar im Supervised-Modus

Account Name	Account Name
Principal Name	Einzigartige Identität an welchem der Kerberos Tickets verteilen darf
Realm	Ihr zu benutzender Kerberos Realm (z.B. Ihre Domain)

Mit dem  Symbol können Sie weitere URLs festlegen.

URL pattern used to limit this account	Festzulegende URLs an welche der Kerberos Tickets verteilen darf
--	--

Mit dem  Symbol können Sie weitere Apps festlegen.

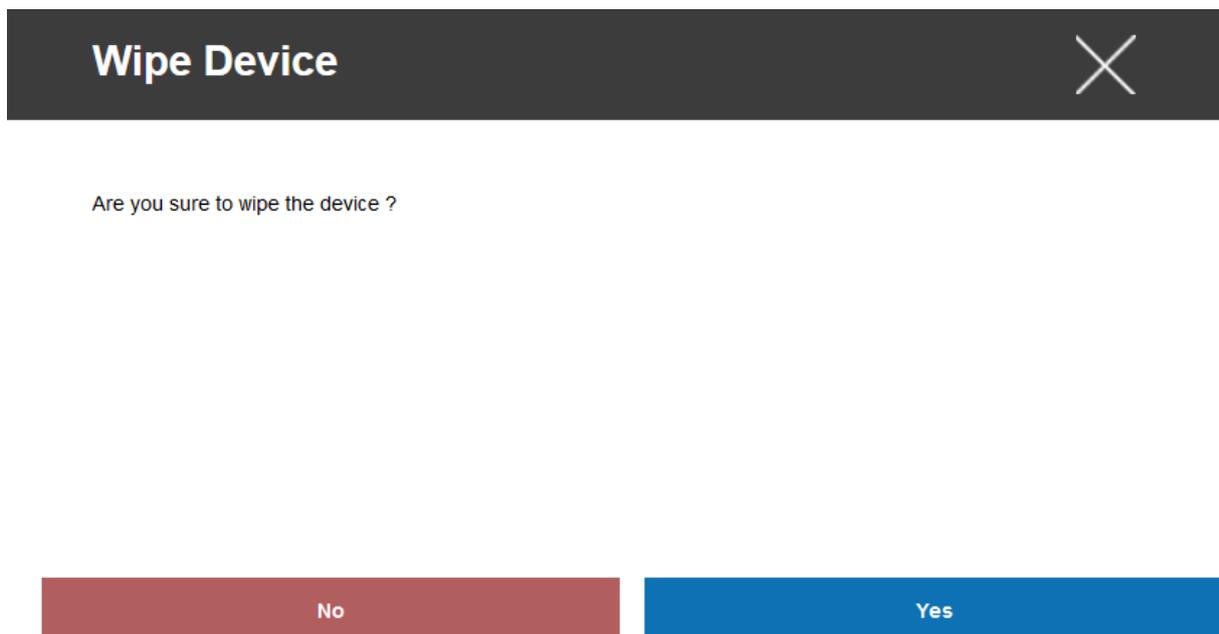
Apps to limit this account	Festzulegende Apps an welche der Kerberos Tickets verteilen darf
----------------------------	--

End of Life (nur auf Device Ebene)

Wipe (nur auf Device Ebene)

Unter „Wipe“ können Sie das Gerät auf die Werkseinstellungen zurücksetzen, hier werden sowohl die geschäftlichen, als auch die privaten Daten auf dem Endgerät gelöscht

Mit dem Klick auf das „Minussymbol“  sollten Sie folgende Meldung erhalten



Mit „Yes“ können Sie die *Löschung durchführen*.

Unter „Wipe Report“ können Sie sich folgende Dinge anzeigen lassen

Wiped by	Historie von wem der Wipe ausgeführt wurde
Date	Datum
Status	Status (z.B. ob der Wipe erfolgreich durchgeführt wurde)

Restriction Settings

Device Functionality

Sperrern Sie hier einzelne Funktionalitäten des Endgerätes

Allow installing apps	Installation von Apps zulassen
Allow camera	Verwendung der Kamera zulassen
Allow FaceTime	FaceTime zulassen
Allow screen capture	Bildschirmfoto erlauben
Allow auto sync while roaming	Automatische Synchronisierung beim Roaming zulassen
Allow Siri	Siri erlauben
Allow voice dialing	Sprachwahl erlauben
Allow in-app purchase	App-interne Käufe erlauben
Require iTunes Store password for all purchases	Es findet für alle Apps immer eine Passwortabfrage statt
Allow multiplayer gaming	Mehrspielermodus erlauben
Allow adding Game Center friends	Hinzufügen von Game Center-Freunden zulassen
Allow open from managed to unmanaged	Öffnen von Content in managed Apps in unmanaged Apps zulassen
Allow open from unmanaged to managed	Öffnen von Content in unmanaged Apps in managed Apps zulassen
Allow today view in lock screen	Wenn diese Einstellung aktiv ist, wird die „Heute“ Ansicht im Notification Center auf dem Sperrbildschirm angezeigt
Allow control center in lock screen	Control Center auf dem Sperrbildschirm erlauben
Allow TouchID	Touch ID zulassen
Allow over-the-air PKI updates	Over-the-air PKI Updates zulassen
Allow passbook while locked	Passbook bei Gerätesperre erlauben
Limit Ad Tracking	Diese Funktion deaktiviert das Ad Tracking (z.B. können Werbeanbieter das Ad Tracking nicht nutzen um personalisierte Werbung zu verteilen)
Allow Handoff	Handoff zulassen
Allow internet results in spotlight	Suchergebnisse in der Spotlight Suche zulassen (z.B. Bing od. Wikipedia)
Require passcode on first AirPlay pairing	Passwort bei erster AirPlay-Verbindung erfordern

Verfügbar im Supervised-Modus

Allow Account Modification	Änderungen an den „Mail,Kontakte,Kalender“ Einstellungen zulassen
Allow AirDrop	AirDrop zulassen
Allow App Cellular Modification	Diese Einstellung blockiert die Änderung welche Apps mobile Daten nutzen darf Diese Einstellung kann z.B. zuerst am Endgerät händisch angelegt werden und anschließend diese Restriktion aktiviert werden
Allow Siri querying user-generated content from the web	Websuche auf bestimmten Webseiten wird verhindert, z.B. Wikipedia weil hier jeder beliebige Änderungen vornehmen kann
Enable Siri profanity filter	Schimpfwörter, welche an Siri gerichtet sind, werden zensiert
Allow iBook Store	iBook Store erlauben
Allow iBook Store Erotica	iBook Store Erotika erlauben
Allow modifying Find my Friends settings	Änderungen der Find my Friends Einstellungen zulassen.
Allow Game Center	GameCenter erlauben
Allow Host Pairing	Verbindung zum Computer verbieten
Allow installing configuration profiles	Installation von Konfigurationsprofilen zulassen
Allow Remove App	Löschen von Apps verhindern
Allow iMessage	iMessage erlauben
Allow erase all contents and settings	Löschen aller Inhalte und Einstellungen zulassen
Allow configuring restrictions	Konfiguration von Einschränkungen zulassen
Allow Podcast	Podcasts erlauben
Allow Definition Lookup	Wörterbuch erlauben
Allow Predictive Keyboard	Personalisierte Tastaturvorschläge zulassen
Allow Auto Correction	Autokorrektur erlauben
Allow Spell Check	Rechtschreibüberprüfung erlauben

Applications

Sperren Sie hier einzelne Applikationen des Endgerätes

Allow use of YouTube	Benutzung von YouTube zulassen
Allow use of iTunes Store	Benutzung des iTunes zulassen
Allow use of Safari	Benutzung von Safari zulassen
Enable autofill	Automatisches Ausfüllen aktivieren
Force fraud warning	Betrugswarnung erzwingen
Enable JavaScript	JavaScript aktivieren
Block pop-ups	Pop-Ups unterdrücken
Allow Cookies	Regelt, wann Safari Cookies akzeptiert
Allow explicit content	Explizite Inhalte zulassen.

iCloud

Sperren Sie bestimmte Funktionalitäten mit der iCloud Synchronisierung

Allow backup	Backups erlauben
Allow document sync	Dokumentsynchronisation erlauben
Allow Photo Stream	Photo Stream zulassen
Allow Shared Photo Stream	Geteilten Photo Stream zulassen
Allow Cloud Keychain Sync	Schlüsselbund Synchronisation zulassen
Allow managed apps to store data	Managed Apps erlauben, Daten zu speichern
Allow notes and highlights sync for enterprise books	Synchronisierung von Markierungen & Notizen in Enterprise Books zulassen
Allow backup of enterprise books	Backups für Enterprise Books erlauben

Security and Privacy

Sperren Sie Funktionalitäten im Zusammenhang mit diagnostischen Daten

Allow diagnostic data to be send to Apple	Übermittlung von diagnostischen Daten an Apple zulassen
Allow user to accept untrusted TLS certificates	User erlauben, nicht vertrauenswürdige TLS Zertifikate zu akzeptieren
Force encrypted backups	Verschlüsselte Backups erzwingen

BYOD Container

Activation

Aktivieren Sie die von AppTec360 unterstützten Container-Lösungen

Enable Google Divide Container	Aktivieren des Google Divide Containers
Enable SecurePIM Container	Aktivieren des SecurePim Containers

Sollten Sie den SecurePIM Container aktiviert haben finden Sie unter „Activation“ noch folgende zwei Punkte, ebenfalls werden direkt oben vier weitere Tabs freigeschaltet die im Nachgang beschrieben werden.

License	Lizenzschlüssel von SecurePIM
Support Email Address	Support E-Mail Adresse an die sich die User bei Problemen wenden können

SecurePIM Password

Unter „SecurePIM Password“ können Sie die Richtlinien für die Passwort-Stärke vornehmen.

Session Timeout	Hier können Sie festlegen nach wie viel Minuten das Passwort erneut eingegeben werden muss, nachdem SecurePIM im Hintergrund läuft
Password Length	Passwortlänge um Zugang zum SecurePIM Container zu erhalten
Upper Case Characters	Mindestanzahl an Großbuchstaben
Lower Case Characters	Mindestanzahl an Kleinbuchstaben
Special Characters	Mindestanzahl an Sonderzeichen
Digits	Mindestanzahl an Zahlen
Wipe Application	Anzahl wie oft das Passwort falsch eingegeben werden darf, bis der SecurePIM Inhalt gelöscht wird (Die App bleibt dennoch weiterhin auf dem Endgerät bestehen)

SecurePIM Security

Unter „SecurePIM Security“ können Sie diverse Sicherheitseinstellungen vornehmen.

Detect Jailbroken Devices	Sollte diese Einstellung aktiv sein, wird der Zugang zum SecurePIM Container gesperrt, sobald das Gerät als jailbroken erkannt wird
Secure Text Fields	Der Inhalt der Eingabefelder wird verschlüsselt, keinerlei Informationen gelangen an das Betriebssystem (iOS) Hinweis: Sofern diese Einstellung aktiv ist, ist eine Auto-Korrektur nicht mehr möglich
Export Contact Data to Device	Sollte diese Einstellung aktiv sein, ist es dem User erlaubt die Exchange Kontakte auf sein lokales Gerät zu exportieren Hinweis: Nur der Name und die Telefonnummer werden exportiert
Show Event Location	Sollte diese Einstellung aktiv sein, wird der Ort des bevorstehenden Events in der Benachrichtigungsleiste angezeigt
Show Event Title	Sollte diese Einstellung aktiv sein, wird der Name des bevorstehenden Events in der Benachrichtigungsleiste angezeigt

SecurePIM Browser

<input checked="" type="checkbox"/> On	
Whitelisted URLs +	
http://www.apptec360.com/	-
Blacklisted URLs +	
www.facebook.com	-
Bookmark Title	Bookmark URL +
AppTec English	http://www.apptec360.com/en_home.html -

Hier können Sie den hauseigenen Browser von SecurePIM konfigurieren.

Mit dem  Symbol sind Sie in der Lage ein neue URL zu definieren.

Mit dem  Symbol können Sie eine definierte URL wieder entfernen.

„Whitelisted URLs“ sind URLs die aufgerufen werden dürfen.

„Blacklisted URLs“ sind URLs die nicht aufgerufen werden und somit blockiert werden.

Beachten Sie bitte, dass die Whitelisteinträge höher priorisiert werden als die Blacklisteinträge.

Unter „Bookmark Title“ können Sie einen Titel vergeben, anhand der „Bookmark URL“ können Sie eine URL Adresse dem Bookmark Titel vergeben – somit können Sie individuell Lesezeichen an die jeweiligen User verteilen.

Exchange

Unter „Exchange“ können Sie ein Exchange Konto konfigurieren.

ActiveSync Email Address	Exchange E-Mail Adresse (beachten Sie die „Placeholders“)
ActiveSync Exchange Login	Exchange Benutzernamen (beachten Sie die „Placeholders“)
ActiveSync Exchange Server	Exchange Server Adresse (FQDN)
ActiveSync Exchange Domain	Exchange Domain Adresse
User Certificate	Benutzerzertifikat
Certificate based authentication	Benutzer authentifizieren sich anhand des Zertifikats
Allow S/MIME Encryption	Erlaubt es dem User seine Mails zu verschlüsseln
Allow S/MIME Signing	Erlaubt es dem User seine Mails zu signieren
CRL Check	Falls aktiv wird das private Zertifikat mit der CRL (Certificate Revocation List) abgeglichen

Connection Management

Wifi

Services Set Identifier (SSID)	SSID des zu verbindenden Netzwerks
Auto Join	Automatischen Beitreten zum Netzwerk aktivieren
Hidden Network	Aktivieren, falls der AP die SSID nicht broadcastet
Proxy Setup	Konfigurieren eines Proxy für den Access Point
None	Keinen Proxy festlegen
Manual	Einen Proxy manuell festlegen
Proxy Server URL	Adresse zum Abrufen der Proxy Settings
Port	Port für den Proxy festlegen
Authentication	Username zur Authentifizierung am Proxy
Password	Passwort zur Authentifizierung am Proxy
Automatic	Einen Proxy automatisch festlegen
Proxy Server URL	URL zum Abrufen der Proxyeinstellungen
Security Type	Sicherheitstyp des AP festlegen
WEP	
Password	Passwort für den AP
WPA/WPA2	
Password	Passwort für den AP
WEP Enterprise – WPA / WPA2 Enterprise – Any Enterprise	
Protocols	
TLS	Aktivieren bzw. Deaktivieren
TTLS	Aktivieren bzw. Deaktivieren
LEAP	Aktivieren bzw. Deaktivieren
PEAP	Aktivieren bzw. Deaktivieren
EAP-FAST	Aktivieren bzw. Deaktivieren
EAP-SIM	Aktivieren bzw. Deaktivieren
Authentication	
Username	Username zur Authentifizierung
Don't use Per-Connection Password	Kein Per-Verbindung Passwort verwenden
Identity Certificate	Zertifikat zur Authentifizierung hochladen / auswählen
Outer Identity	Extern sichtbare Identität
Trust	

Trusted Certificate 1	Erstes Vertrautes Zertifikat hochladen
Trusted Certificate 2	Zweites Vertrautes Zertifikat hochladen
Trusted Certificate 3	Drittes Vertrautes Zertifikat hochladen
Trusted Server Certificate Names	Die Namen der zu erwartenden Serverzertifikate (in einer kommagetrennten Liste)
None	Keine Sicherheit festlegen

VPN

Connection Name	Name des VPN-Profiles
VPN Type	
VPN	Der gesamte Netzwerkverkehr des Gerätes wird über die VPN-Verbindung geleitet.
Connection Type	VPN-Verbindungstyp festlegen
IPsec (cisco)	IPsec Protokoll von cisco
PPTP	PPTP Protokoll
L2TP	L2TP Protokoll
Cisco AnyConnect	AnyConnect Protokoll
Juniper SSL	Juniper SSL Protokoll
F5 SSL	F5 SSL Protokoll
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Aruba VIA Protokoll
Custom SSL	Verbindung über Custom SSL
OpenVPN	OpenVPN Protokoll
Per-App VPN	Bei Öffnen einer bestimmten App wird die VPN-Verbindung hergestellt
Automatically start Per-App VPN connection	Bei Start der App wird die VPN-Verbindung automatisch hergestellt
Connection Type	VPN-Verbindungstyp festlegen
Cisco AnyConnect	AnyConnect Protokoll
Juniper SSL	Juniper SSL Protokoll
F5 SSL	F5 SSL Protokoll
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Aruba VIA Protokoll
Custom SSL	Verbindung über Custom SSL
OpenVPN	OpenVPN Protokoll
Proxy Setup	Konfigurieren eines Proxy für die VPN-Verbindung
None	Keinen Proxy festlegen
Manual	Einen Proxy manuell festlegen
Proxy Server URL	Adresse zum Abrufen der Proxy Settings
Port	Port für den Proxy festlegen
Authentication	Username zur Authentifizierung am Proxy
Password	Passwort zur Authentifizierung am Proxy
Automatic	Einen Proxy automatisch festlegen
Proxy Server URL	URL zum Abrufen der Proxyeinstellungen
Show Placeholders	Zeigt alle verfügbaren User-Variablen an, welche AppTec benutzen kann,

APN

Access Point Name	Der Name des Access Points
Access Point User Name	Der Benutzername des AP User
Access Point Password	Password des AP Users
Proxy Server	Adresse des Proxy Servers
Port	Der entsprechende Proxy Port

Cellular

Enable Data Roaming	Aktivieren des Datenroamings
Enable Voice Roaming	Aktivieren des Sprachroamings
Enable Hotspot	Aktivieren des Hotspots erlauben

HTTP Proxy

Proxy Type	
Manual	Einen Proxy manuell festlegen
Proxy Server URL	Adresse zum Abrufen der Proxy Settings
Port	Port für den Proxy festlegen
Authentication	Username zur Authentifizierung am Proxy
Password	Passwort zur Authentifizierung am Proxy
Automatic	Einen Proxy automatisch festlegen
Proxy PAC URL	PAC URL des Proxy
Allow direct connection if PAC is unreachable	Verbindung ohne VPN zulassen, falls der PAC nicht erreichbar ist.
Allow bypassing proxy to access captive networks	Erlauben, an dem Proxy vorbei, sich zu internen Netzwerken zu verbinden.

AirPrint

IP Address	IP-Adresse des Druckers
Resource Path	Eindeutiger Pfad zum AirPrint Gerät

AirPlay

Device Name	Name des Gerätes
Password	Passwort zum Verbinden
Whitelist	Definieren Sie eine Liste an Geräten, mit welchen sich das Gerät ausschließlich verbinden darf

PIM Management

Exchange Active Sync

Account Name	Name des Email Accounts
Exchange ActiveSync Host	Adresse/FQDN des Servers
Allow Move	Das Bewegen von Mails zulassen
Use Only in Mail	Interaktionen dürfen nur in der nativen Mail App stattfinden
Use SSL	Benutze die SSL Verschlüsselung
Domain	Domäne des Servers
User	Benutzername
eMail Address	eMail Adresse (nur auf Device Ebene)
Password (nur auf Device Ebene)	Passwort des Benutzers
Identity Certificate	Wählen Sie das entsprechende Zertifikat zur Authentifizierung am Server aus
Past Days of Mail to Sync	Anzahl an Tagen, bis zu welchen die Mails zurücksynchronisiert werden sollen. No Limit = Keine Begrenzung
Enable S/MIME	S/MIME Verschlüsselung aktivieren
Signing Certificate	Das entsprechende Signing Certificate hochladen
Encryption Certificate	Das entsprechende Encryption Certificate hochladen

eMail

Einrichten von POP3 / IMAP Konten am Endgerät

Account Description	Name des Email Accounts
Account Type	
IMAP	
Path Prefix	Der Pfad Prefix für spezielle Ordner
POP	
User Display Name	Angezeigter Benutzername
Email Address	Email Adresse des Benutzers
Allow Move	Das Bewegen von Mails zulassen
Enable S/MIME	S/MIME Verschlüsselung aktivieren
Signing Certificate	Das entsprechende Signing Certificate hochladen
Encryption Certificate	Das entsprechende Encryption Certificate hochladen

Incoming Mail	Eingehende Servereinstellungen
----------------------	--------------------------------

Mail Server Address	Adresse des Mail Servers
Mail Server Port	Port des Mail Servers
User Name	Entsprechender Benutzername
Authentication Type	Authifizierungsmethode
None	Keine Authentifizierungsmethode
Password (nur auf Device Ebene)	Passwortabfrage
MDM Challenge-Response	
NTLM	NTLM-Authentifizierung
HTTP MD5 Digest	
Use SSL	Aktivieren, falls SSL benötigt

Outgoing Mail	Ausgehende Servereinstellungen
Mail Server Adress	Adresse des Mailservers
Mail Server Port	Port des Mail Server
User Name	Entsprechender Benutzername
Authentication Type	
None	Keine Authentifizierungsmethode
Password (nur auf Device Ebene)	Passwortabfrage
MDM Challenge-Response	
NTLM	NTLM-Authentifizierung
HTTP MD5 Digest	
Use SSL	Aktivieren, falls SSL benötigt
Outgoing password same as incoming	Ausgehendes Passwort entspricht dann dem eingehenden Passwort
Use only in mail	Aktivieren, falls ausgehende Nachrichten nur über die Mail-App versendet werden sollen

CalDav

Einrichtung und Verteilung eines CalDav Accounts konfigurieren

Account Description	Angezeigter Name des Accounts
Hostname	Hostname bzw. IP Adresse
Port	Port des CalDav Accounts
Principal URL	Principal URL des Accounts
Username	Entsprech. CalDav Benutzername
Password (nur auf Device Ebene)	Entsprech. CalDav Passwort
Use SSL	Aktivieren, falls SSL benötigt

CardDav

Einrichtung und Verteilung eines CardDav Accounts konfigurieren

Account Description	Angezeigter Name des Accounts
Hostname	Hostname bzw. IP Adresse
Port	Port des CalDav Accounts
Principal URL	Principal URL des Accounts
Username	Entsprech. CardDav Benutzername
Password (nur auf Device Ebene)	Entsprech. CardDav Passwort
Use SSL	Aktivieren, falls SSL benötigt

Subscribed Calendars

Einrichtung und Verteilung von Subscribed Calendars

Description	Angezeigter Name des Accounts
URL	URL der Kalenderdatei
Username	Benutzer des Kalenderabos
Password (nur auf Device Ebene)	Passwort des Kalenderabos
Use SSL	Aktivieren, falls SSL benötigt

LDAP

Richten Sie an dieser Stelle eine LDAP-Verbindung ein, um einen dynamischen Zertifikatsaustausch zwischen Endgerät und Active Directory zu erlauben. Beachten Sie, dass der benutzte User entsprechende Leseberechtigungen benötigt.

Account Description	Beschreibung des Accounts
Account Username	Benutzer für den LDAP-Zugriff
Account Password	Passwort für den LDAP-Zugriff
Account Hostname	Hostname/IP Adresse des LDAP Servers
Use SSL	Aktivieren, falls SSL benötigt

Im zweiten Abschnitt können Sie noch die einzelnen Filter zur Suche im LDAP Verzeichnis definieren.

Description	Scope	Search Base
Beschreibung des Filters	Suchlevel im LDAP Verzeichnis	Definieren der einzelnen Filter

Web Managment

Webclips

Definieren Sie an dieser Stelle Lesezeichen mit Links zu Webseiten, Intranetportalen etc, welche daraufhin als Applikation auf dem Endgerät zu sehen sein werden.

Label	Name der Verknüpfung auf dem Endgerät
URL	Link zur entsprechenden Website
Removeable	Wenn aktiviert, kann der User den Webclip entfernen
Icon	Laden Sie über diesen Dialog ein Logo für die Verknüpfung hoch: Maße 180x180, Format png
Precomposed Icon	Wenn aktiviert, werden keine zusätzlichen Effekte (Schatten, Glanz) auf dem Icon angezeigt
Full Screen	Bei Öffnen des Webclips öffnet sich der Browser im Vollbildschirmmodus

Web Content Filter

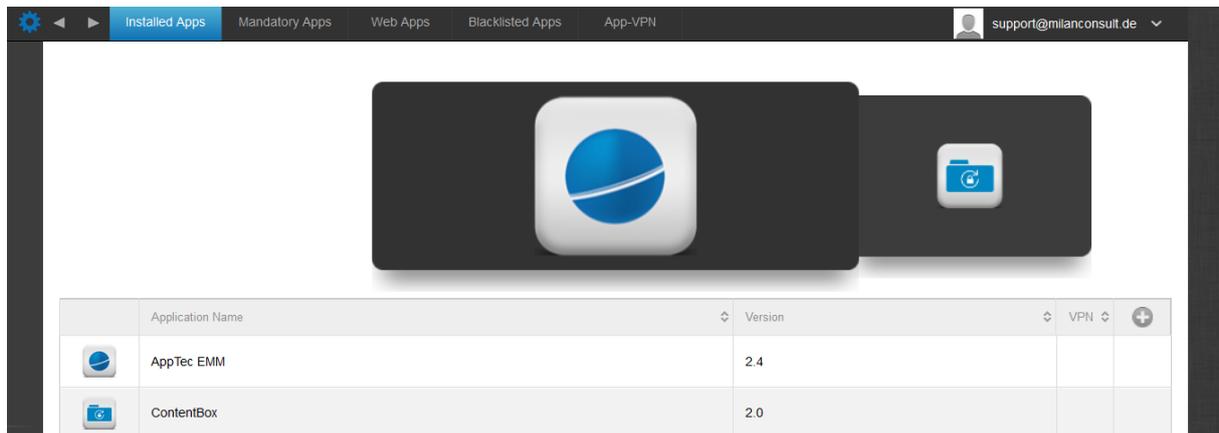
Der Web Content Filter ermöglicht es, Zugriff auf bestimmte Internetseiten zu begrenzen.

Allowed Websites	
Limit Adult Content	Es wird automatisch ein Webfilter für nicht jugendfreie Inhalte angewandt
Permitted URLs	Fügen Sie über das + Symbol entsprechende zugelassene Seiten hinzu
Blacklisted URLs	Fügen Sie über + Symbol entsprechende gesperrte Seiten hinzu
Specific Websites Only	Es können nur die definierten Inhalte angezeigt werden, welche Sie über das + Symbol hinzufügen können.

App Management

Enterprise App Manager

Installed Apps (nur auf Device Ebene)



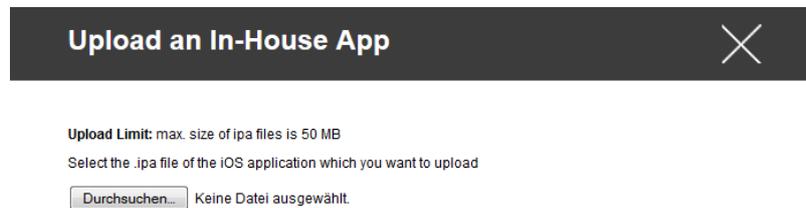
Über das  Symbol lassen sich direkt neue Apps auf das Endgerät pushen.

Sie können sowohl eine „Apple AppStore“ App aus dem öffentlichen AppStore auf das Gerät pushen, als auch eine eigenentwickelte In-House App.

Oder Sie wählen unter der Kategorie „iOS In-House Apps“ einer Ihrer unter den General Settings hochgeladene In-House App aus.

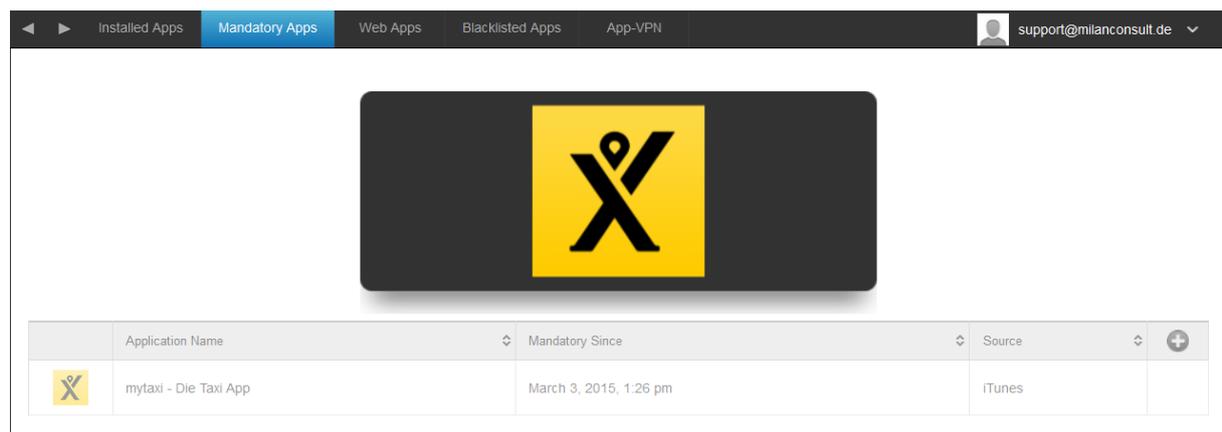
Bitte beachten Sie dass dies nur ein einmaliger Befehl ist, sollte dieser aus welchen Gründen auch immer an Endgerät nicht ankommen, findet keine Wiederholung statt!

Sie können auch direkt über „Upload In-House App“ eine ipa Datei auswählen und diese hochladen.



Mandatory Apps

Unter den Mandatory Apps können Sie zwingend erforderliche Apps festlegen. Der User wird ständig dazu aufgefordert sich diese besagte App zu installieren. Über das  kann direkt eine zwingend erforderliche App definiert werden.

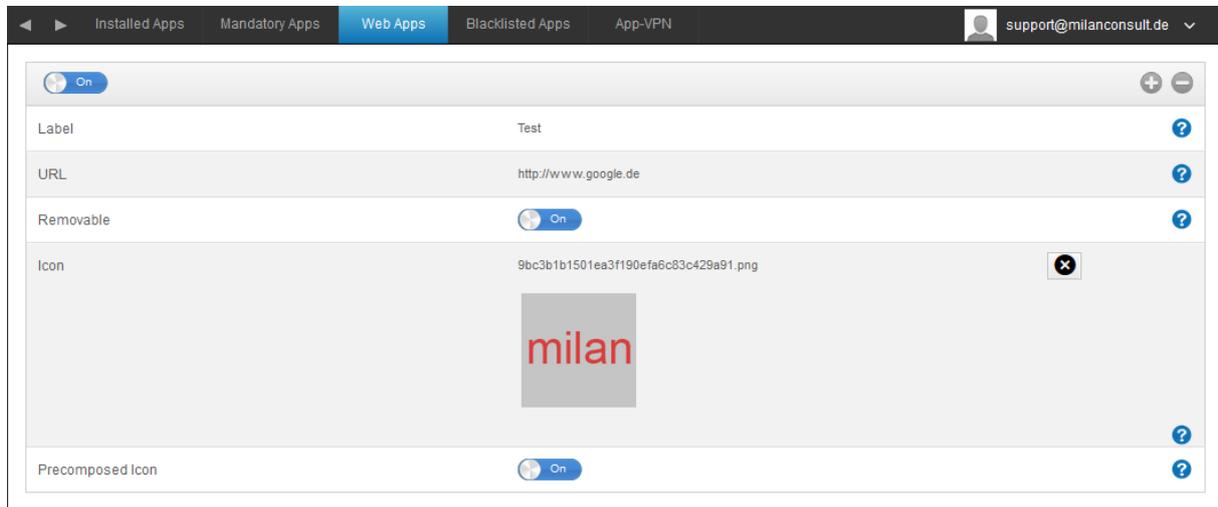


Dies kann wie bei den „Installed Apps“ eine Apple App Store App sein, aber auch eine In-House App.

Sollte es sich um ein Supervised Gerät handeln, wird die App automatisch installiert. Die Bedienung findet gleich statt wie beim Punkt Installed Apps.

Web Apps

Unter dem Punkt „Web Apps“ können, ähnlich wie bei den „Web Clips“ im Bereich Web Management, Internetseiten oder Intranetportale als Applikation auf das Endgerät gepusht werden, standardmäßig werden Web Apps im Vollbildschirm angezeigt, bei den Webclips ist dies einstellbar.



Label	Name der Verknüpfung auf dem Endgerät
URL	Link zur entsprechenden Website
<u>Removeable</u>	Wenn aktiviert, kann der User den Webclip entfernen
Icon	Laden Sie über diesen Dialog ein Logo für die Verknüpfung hoch: Maße 180x180, Format png
Precomposed Icon	Wenn aktiviert, werden keine zusätzlichen Effekte (Schatten, Glanz) auf dem Icon angezeigt

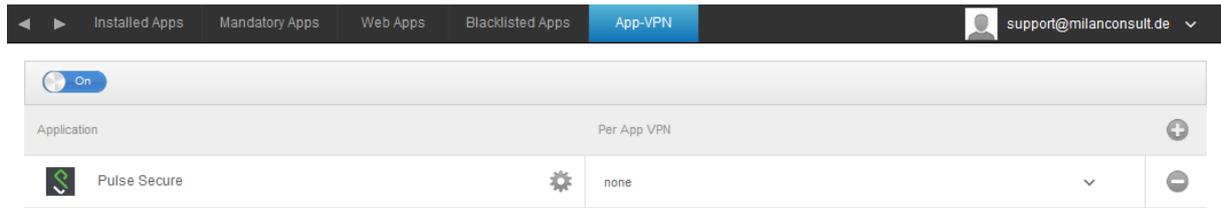
Blacklisted Apps

Hier können Sie, abgesehen vom App Store, die entsprechenden iTunes Store deaktivieren

Block iTunes Apps	Alle AppStore Apps werden deaktiviert bzw. versteckt
-------------------	--

App-VPN

Über das  Symbol können Sie Applikationen definieren, welche beim Starten automatisch die ausgewählte VPN-Verbindung aufbauen.



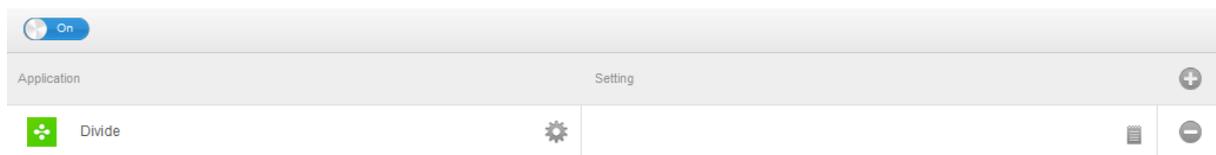
App Settings

Unter „App Settings“ können Sie einer App (sofern die App das unterstützt, fragen Sie ggf. beim Hersteller der App nach) bestimmte Werte im Vorfeld mitgeben.

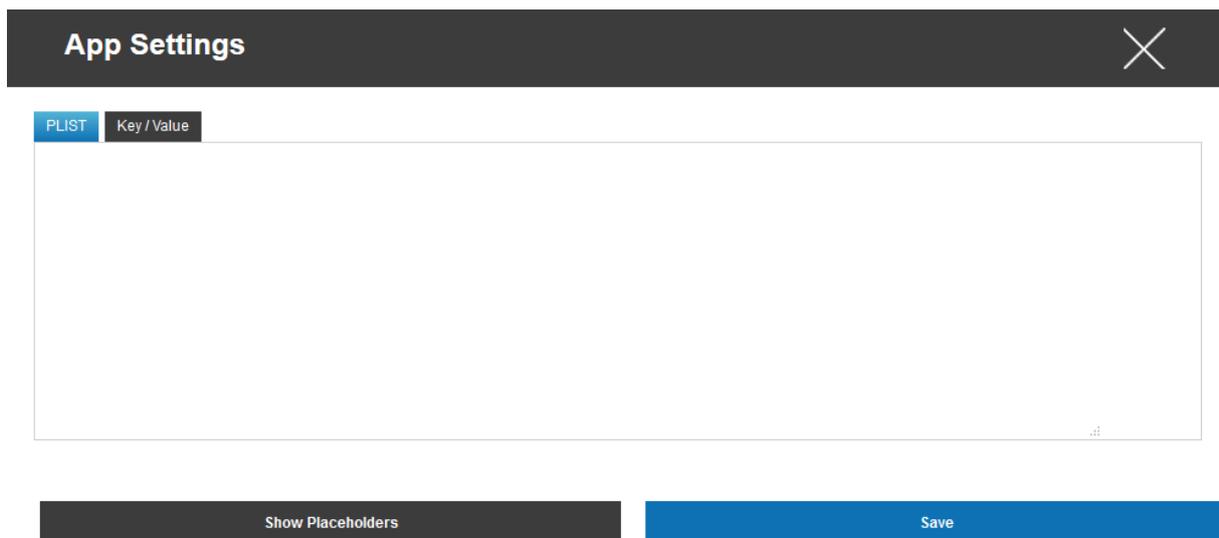
Über das  Symbol können Sie eine (weitere) App hinzufügen. Sie finden die gewohnte AppTec Darstellung eines App-Imports wieder.

Suchen Sie hier nach der App die Sie gerne konfigurieren möchten und wählen Sie diese aus.

Sollte der Import erfolgreich gewesen sein, erhalten Sie folgende Ansicht:

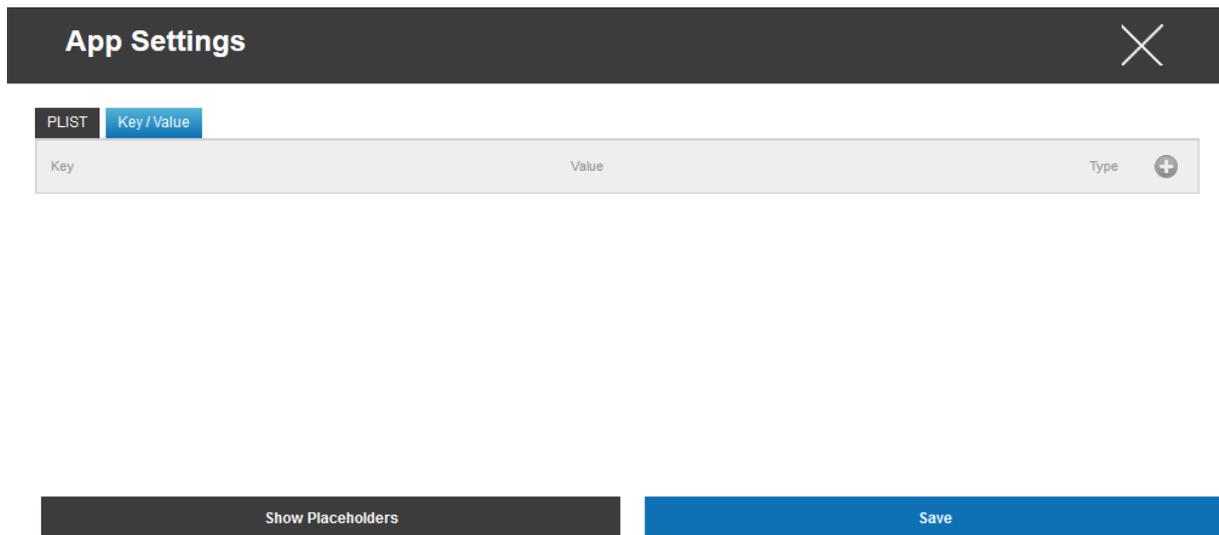


Sie können nun mit einem Klick auf das  diverse Anpassungen vornehmen. Folgende Übersicht werden Sie dann erhalten:

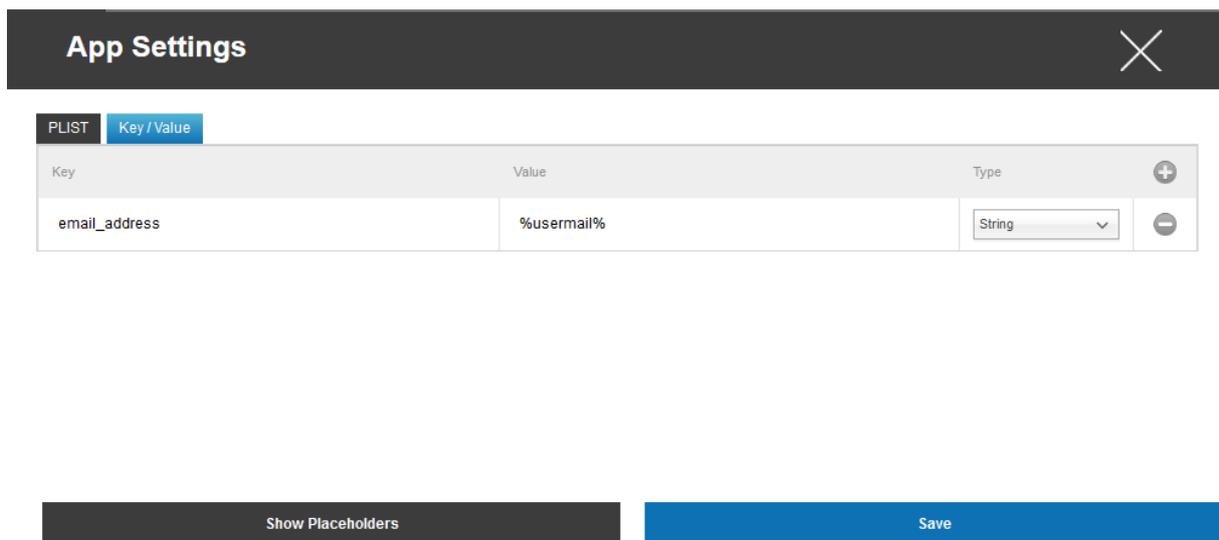


Sollten Sie bereits eine vorhandene PLIST (Quelltext der Konfiguration) haben, können Sie diesen hier einfügen und mit „Save“ das ganze abspeichern.

Unter „Key / Value“ können Sie der App spezifische Konfigurationen mitgeben.



Hier können Sie mit dem  Symbol einen neuen Key und den dazu gehörigen Wert (Value) setzen.



Selbstverständlich stehen Ihnen alle Platzhalter von AppTec zur Verfügung.

Erklärung der „Type“:

String	Text
Boolean	True/False (wahr / falsch)
Number	Nummer

Mit dem  Symbol können Sie eine App wieder entfernen.

Enterprise App Store

iTunes Apps

Unter diesem Punkt können Sie optionale Apps für Ihre User verteilen. Sollte sich hier eine App befinden, wird automatisch auf dem Endgerät der AppTec Store installiert.

Dies sind lediglich Verlinkungen auf den offiziellen Apple App Store, aus diesem Grund muss auf jedem Endgerät eine Apple ID hinterlegt sein. Wir empfehlen an dieser Stelle, dass jeder User seine eigene Apple ID besitzt.

Mit dem  können Sie weitere Apps hinzufügen.

Application Name	Version	
------------------	---------	---

Danach sollte sich ein Fenster mit folgender Übersicht öffnen.

Bitte beachten Sie, dass nur kostenlose Apps angezeigt werden, kostenpflichtige Apps werden nur über das VPP angezeigt.

Select an application

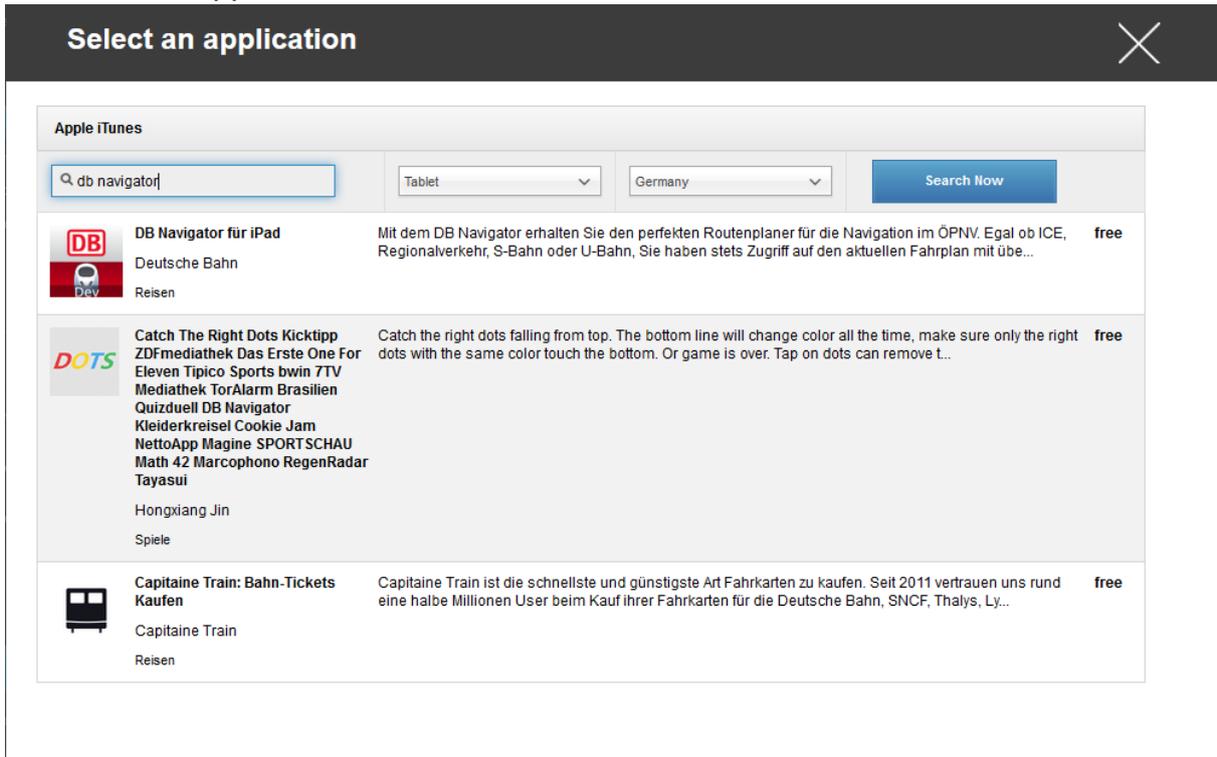

Apple iTunes

Tablet

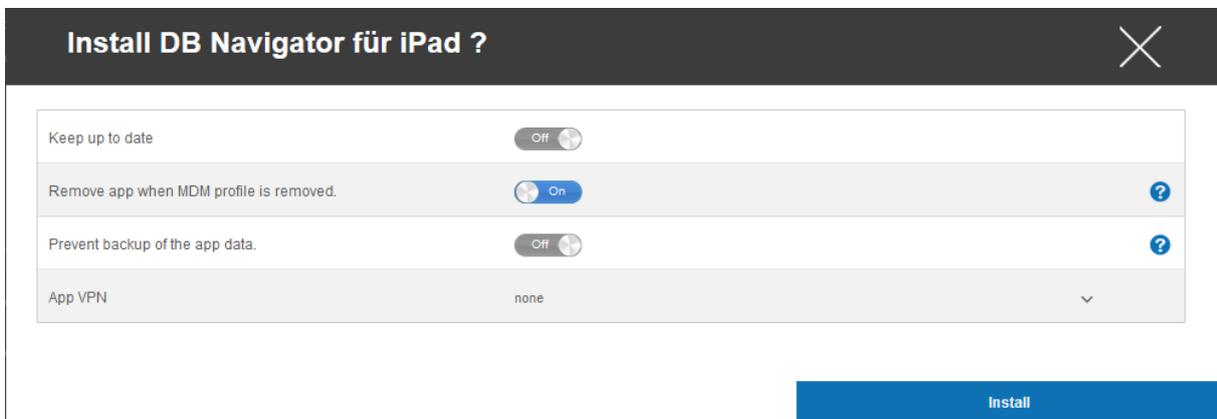
Germany

Search Now

Bei „Enter Searchterm here ...“ können Sie nach einer sich im Apple App Store befindenden App suchen.



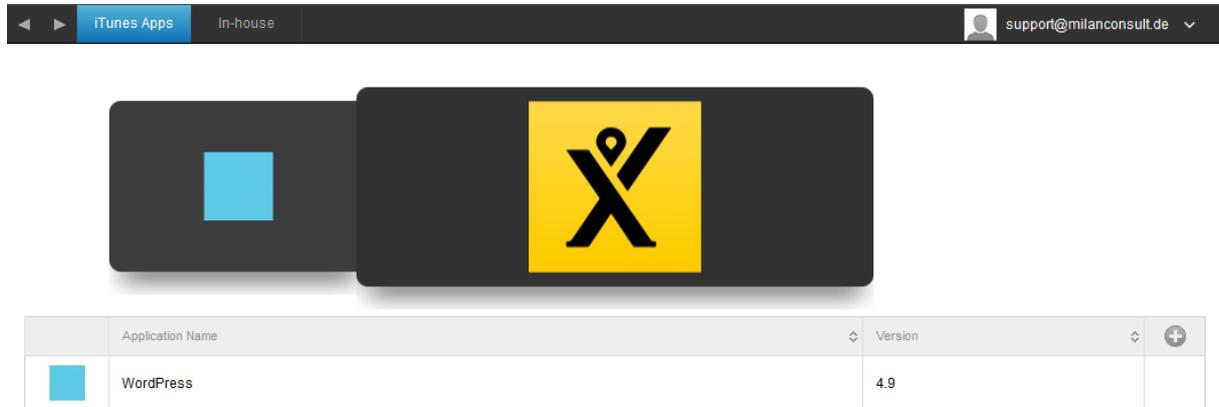
Wenn Sie nun auf das Icon oder auf den Name der App klicken, werden Sie nochmals gefragt, weitere Einstellungen vorzunehmen...



Keep up to date	Es wird binnen einer Woche überprüft, ob ein Update für die App vorhanden ist, falls ja wird dieses Update installiert
Remove app when MDM profile is removed	Bei Entfernung der Geräteverwaltung wird die App deinstalliert
Prevent backup of app data	Es wird kein Backup von app-spezifischen Daten erstellt
App-VPN	VPN-Verbindung auswählen, welche bei Öffnen der App startet

Nach einem Klick auf „Install“ wird die App in den Enterprise App Store hinzugefügt und kann dann vom Endgerät über den AppTec AppStore installiert werden

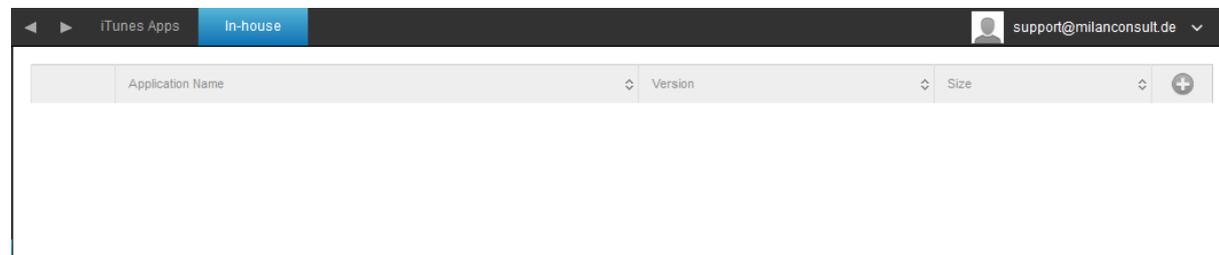
Sollte der App-Store Import erfolgreich gewesen sein, erhalten Sie folgende Übersicht:



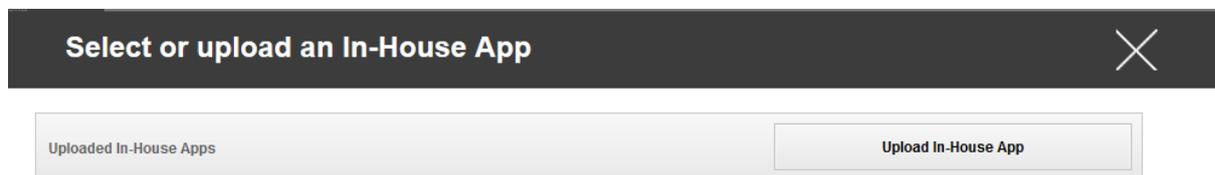
In-House

Unter dem Punkt „In-House“ können Sie Ihre eigenentwickelten Apps hochladen und verteilen.

Mit dem  können Sie weitere In-House Apps verteilen.



Sollten Sie bisher noch keine In-House App verteilt haben, erhalten Sie nun folgende Übersicht:

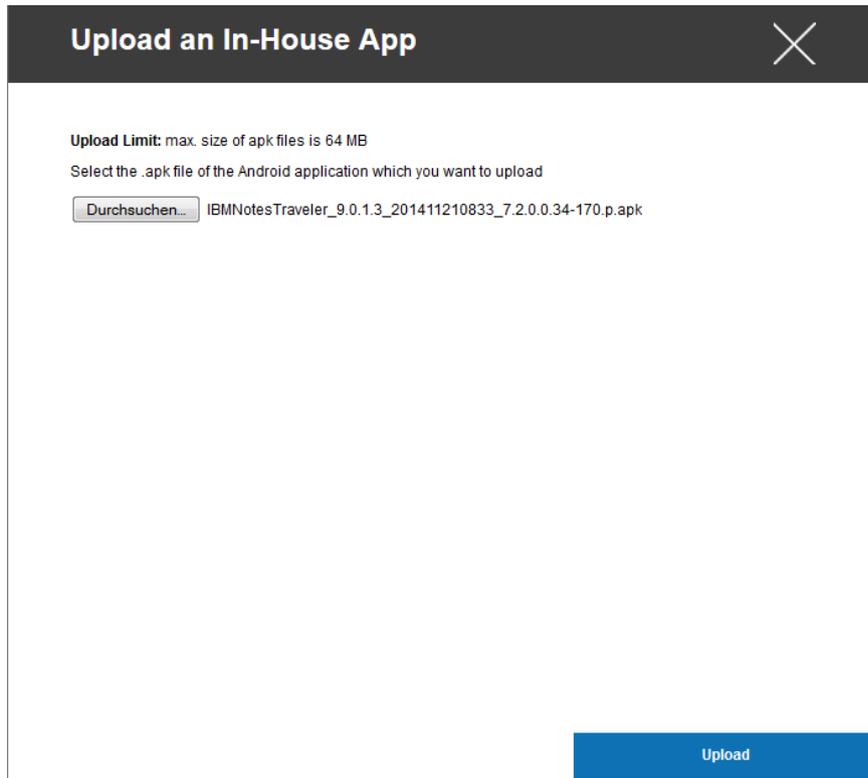


Klicken Sie hierzu auf „Upload In-House App“, nun erhalten Sie folgende Übersicht:

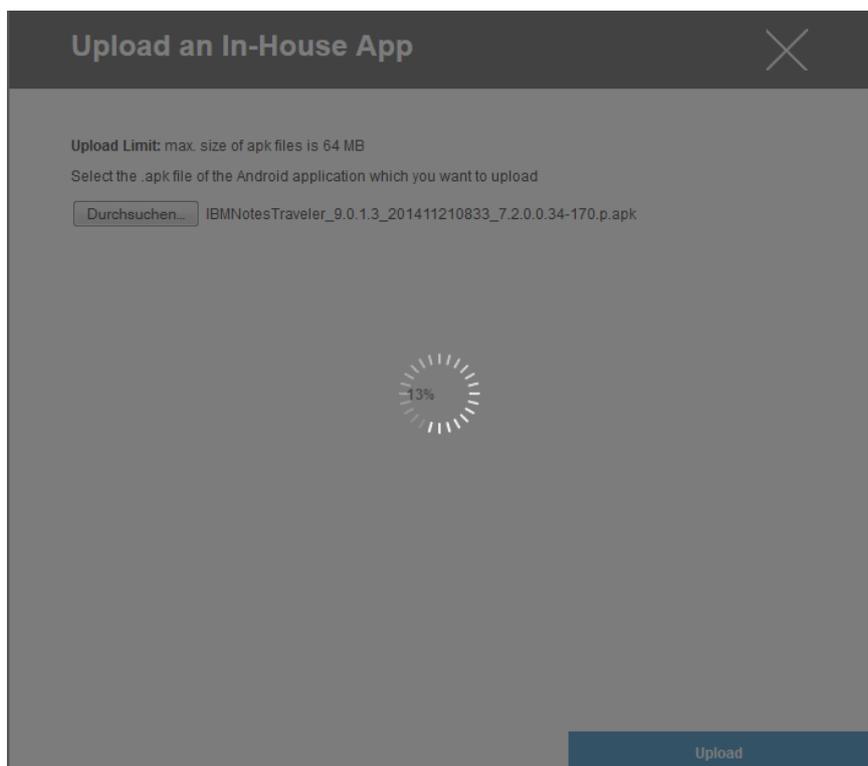


Upload Limit: max. size of ipa files is 50 MB
 Select the .ipa file of the iOS application which you want to upload
 Keine Datei ausgewählt

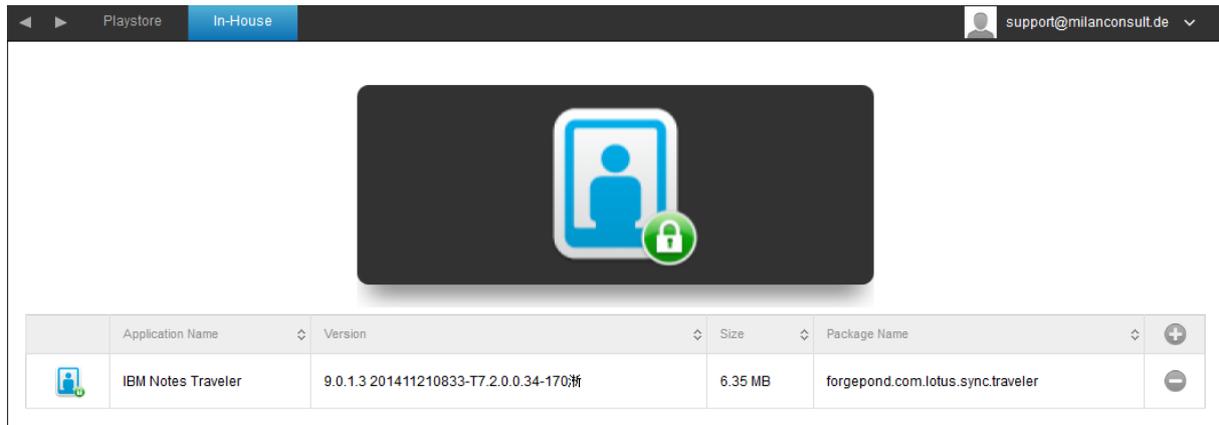
Wählen Sie nun mit „Durchsuchen...“ eine .ipa Datei aus und klicken Sie anschließend auf „Upload“.



Ihre App wird nun hochgeladen, in der Mitte des Kreises können Sie eine Prozentanzahl sehen wie weit Ihre App bereits hochgeladen ist.



Sollte ein Upload der In-House App erfolgreich gewesen sein, sehen Sie nun die eben hochgeladen App in ihrem App Katalog.



Der User ist nun in der Lage, auf seinem Endgerät diese App im AppTec Store unter der Kategorie „In-House“ sehen und installieren zu können.

Da es sich hierbei um keine öffentliche Apple AppStore App handelt, braucht der User an seinem jeweiligen Endgerät keine hinterlegte Apple ID.

Kiosk Mode

Der Kiosk Mode erlaubt es Ihnen eine App oder URL vorzudefinieren, dann ist es ausschließlich möglich diese App bzw. URL auszuführen/besuchen.

Ebenfalls können Sie im Kiosk Mode diverse Hardwaretasten deaktivieren.

Verfügbar im Supervised Modus	
Application Type	Package
	URL
Package	Wenn Sie eine App im Kiosk Mode starten möchten, wählen Sie unter „Application Type“ „Package“ aus
Kiosk Application	Klicken Sie hier, um eine App die im Kiosk Mode gestartet werden soll auszuwählen Sie finden die gängige Übersicht vom App Management vor Sie können zwischen „Apple iTunes Apps“, und „iOS In-House Apps“ wählen
URL	Wenn Sie eine URL im Kiosk Mode starten möchten, wählen Sie unter „Application Type“ „URL“ aus
URL	Definieren Sie hier nun Ihre gewünschte URL Adresse
Same Origin Policy	Sollte diese Funktion aktiviert sein, kann der User nur unter Unterseiten der vordefinierten URL surfen z.B. haben Sie folgende URL definiert: www.mypage.com der User kann dann auf www.mypage.com/subpage surfen
Whitelisted URLs	Hier können Sie eine Whitelist pflegen, alle diese URLs sind zulässig Maximal 1 URL pro Linie Eine URL muss mit http:/ oder https:// beginnen
Blacklisted URLs	Hier können Sie eine Blacklist pflegen, alle diese URLs sind unzulässig Maximal 1 URL pro Linie Eine URL muss mit http:/ oder https:// beginnen
Clear Browser after inactivity	Nach Inaktivität wird der Browser Cache geleert
Exit Password Enabled	Wenn Sie diese Funktion aktivieren, ist es dem User möglich, mit den von Ihnen vordefinierten Passwort den Kiosk Mode beenden zu können
Exit Password	Dies ist das von Ihnen vordefinierte Passwort
	Sie können anhand der Uhrzeit den

Scheduled Kiosk Mode	Kiosk Mode planen, dieser wird dann in der von Ihnen definierten Uhrzeit automatisch gestartet und beendet
Start Time	Startzeit
Time in minutes	Zeit in Minuten, nachdem der Kiosk Mode wieder beendet werden soll
Disable Touch	Falls aktiviert, so wird der Touchscreen deaktiviert
Disable Device Rotation	Falls aktiviert, so wird die automatische Bildschirmanpassung deaktiviert
Disable Ringer Switch	Falls aktiviert, so wird der Ringer Switch deaktiviert. Das Verhalten ist daraufhin abhängig von der zuvor eingestellten Funktion
Disable volume buttons	Falls aktiviert, so werden die Lautstärkeknöpfe deaktiviert
Disable Sleep Wake Button	Falls aktiviert, so wird der An/Aus Schalter deaktiviert
Disable Auto Lock	Falls aktiviert, so wird das Gerät nicht automatisch in den Standby gesetzt
Enable Voice Over	Falls aktiviert, so wird der Voice Over Assistent aktiviert
Enable Zoom	Falls aktiviert, so wird der Zoom aktiviert
Enable Invert Colors	Falls aktiviert, so wird der invertierte Displaymodus aktiviert
Enable Assistive Touch	Falls aktiviert, so wird der AssistiveTouch aktiviert
Enable Speak Selection	Falls aktiviert, so wird die Sprachauswahl aktiviert
Enable Mono Audio	Falls aktiviert, so wird Mono Audio aktiviert
VoiceOver	Falls aktiviert, kann der User VoiceOver anpassen
Zoom	Falls aktiviert, kann der User den Zoom anpassen
Invert Colors	Falls aktiviert, kann der User die invertierten Farben anpassen
Assistive Touch	Falls aktiviert, kann der User Assistive Touch anpassen.

Content Management

ContentBox

Hier können Sie die ContentBox aktivieren bzw. deaktivieren

Enable ContentBox	ContentBox aktivieren
-------------------	-----------------------

Konfiguration Android

Je nachdem ob Sie aktuell ein Profil oder ein Gerät ausgewählt haben, unterscheidet sich die Darstellung und deren Unterpunkte – bitte beachten Sie dies sorgfältig!

General

Profile Overview (nur auf Profil Ebene)

Sollten Sie sich in einem Profil befinden, erhalten Sie hier einen kurzen Überblick über das Profil in Bezug auf Name, OS, Erstellungsdatum, Autor, etc.

Profile Name	Name des Profils – kann direkt hier umbenannt werden
Operating System	Für welches Betriebssystem das Profil gilt
Created At	Erstelldatum
Created By	Ersteller des Profils
Profile Revision	Anzahl wie oft das Profil bereits geändert wurde

Device Overview (nur auf Device Ebene)

Sollten Sie sich auf einem Gerät befinden, erhalten Sie hier eine zusammenfassende Übersicht des ausgewählten Geräts, folgendes ist hier enthalten:

Device Name	Name des Geräts
Phone Number	Telefonnummer des Geräts
OS Version	OS Version des Geräts
Operating System	Betriebssystem (Android / iOS / Windows Phone)
Serial Number	Seriennummer des Geräts
Device Ownership	Firmen oder Privatgerät
Device Typ	Telefon oder Tablet
Rooted	Status ob das Gerät gerootet wurde
Compliant	Den Richtlinien entsprechend
Last Seen	Zeitpunkt an dem sich das Gerät zuletzt mit AppTec verbunden hat

Config Revision

Hier erhalten Sie eine Übersicht welches Gruppenprofil dem Gerät zugewiesen ist. Wenn sie auf das Gruppenprofil klicken, kommen Sie direkt zu diesem Profil und können Einstellungen vornehmen.

Mit dem  Symbol können Sie die zugewiesenen Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Mit dem  Symbol können Sie alle getätigten Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Device Log

Hier erhalten Sie diverse Gerätelogs.

Gegebenenfalls können Sie bei einem Fehler hier direkt die Ursache ausfindig machen.

Device Settings

Client Configuration

Hier können Sie folgende Einstellung für Ihr Android Gerät vornehmen:

Warning message after disabling Device Management	Festgelegte Warnmeldung, sobald der AppTec Geräteadministrator deaktiviert wird
Enforcement action after disabling Device Management	Die Aktion die ausgeführt werden soll, sobald der Geräteadministrator deaktiviert wird: → do nothing = keine Aktion → Lock Device = Gerät sperren → Wipe Device = Gerät wird auf die Werkseinstellungen zurückgesetzt
Out of Compliance Time	Zeitlimit, nach welchem die "Enforcement Action after compliance" durchgeführt wird, falls das Gerät nicht compliant ist. Min. 1 Minute Max. 24 Stunden
Enforcement action after compliance timeout	Die Aktion die ausgeführt werden soll, sobald ein Gerät nicht mehr compliant ist. → do nothing = keinerlei Aktionen → Lock Device = Gerät sperren → Wipe Device = Gerät wird auf die Werkseinstellungen zurückgesetzt
Data Collection Frequency	Frequenz in welcher Geräte- und GPS-Informationen gesammelt werden
Device Heartbeat Frequency	Intervall in welchem sich das Gerät beim AppTec Server meldet Min. 1 Minute Max. 24 Stunden
Enable Location Updates	Falls aktiviert, sendet das Gerät Standortinformationen an den AppTec Server
Location Update Time	Bestimmt, in welchem Zeitintervall das Gerät Standortinformationen an AppTec übermitteln soll
Use Network Location for Location Update	Wenn aktiviert, so wird die Netzwerklokalisierung zur Standortbestimmungen benutzt (falls dies unter „Restrictions“ deaktiviert wurde, greift diese Einstellung nicht)
Use GPS Location for Location Update	Falls aktiviert, wird GPS für die Standortübermittlung benutzt
Allow Mock (Fake) Locations	Erlaubt das Fälschen der Standortinformation durch Apps Dritter.

Asset Management (nur auf Device Ebene)

Asset Management (nur auf Device Ebene)

Device Info

Model	Modellbezeichnung des Geräts
Operating System	Betriebssystem
OS Version	Betriebssystem Version
Serial Number	Seriennummer
Device Name	Gerätename
Battery Status	Batterieanzeige
Free / Total Memory	Freier / insgesamt Speicherplatz
Samsung Safe	SAFE Schnittstelle von Samsung, nötig für diverse Einstellungsmöglichkeiten
SD Card Available	SD Karte verfügbar
SD Card Emulated	Emulierte SD Karte auf dem Gerät
SD Card Removable	SD Karte kann entfernt werden
SD Free / Total Memory	Freier / insgesamt Speicherplatz der SD Karte

Wi-Fi

IP Address	IP Adresse des Gerätes
WiFi MAC	WiFi MAC Adresse

Cellular

Status	Status (SIM Karte vorhanden)
Phone Number	Telefonnummer
Roaming (Voice / Data)	Romaing Status für Anrufe / Daten
Roaming Status	Aktueller Roaming Status
IP Address	IP Adresse
Operator/Carrier	Mobilfunk Anbieter
Cellular Technology	Genutzter Mobilfunkstandard
IMEI	IMEI Nummer
ICCID	Dies ist die ID der SIM-Chipkarte, oft auch als Smartcard oder Integrated Circuit Card (ICC)
IMSI	Die International Mobile Subscriber Identity (IMSI; deutsch Internationale Mobilfunk-Teilnehmerkennung) dient in GSM- und UMTS-Mobilfunknetzen der eindeutigen Identifizierung von Netzteilnehmern Die IMSI besteht aus maximal 15 Ziffern

	<p>und setzt sich folgendermaßen zusammen:</p> <ul style="list-style-type: none"> • Mobile Country Code (MCC), 3 Ziffern • Mobile Network Code (MNC), 2 oder 3 Ziffern • Mobile Subscriber Identification Number (MSIN), 1-10 Ziffern
Current MCC/MNC	Siehe „SIM MCC/MNC“
SIM MCC/MNC	<p>Der Mobile Country Code ist eine von der ITU im Standard E.212 festgelegte Länderkennung, die zusammen mit dem Mobile Network Code (MNC) zur Identifizierung eines Mobilfunknetzes verwendet wird.</p> <p>Heißt das ist der Ländercode bzw. Mobile Network Code der Simkarte.</p> <p>Wenn man in ein anderes Mobilfunknetz geht sind deshalb logischerweise der „Current MCC/MNC“ und „SIM MCC/MNC“ unterschiedlich.</p>

Bluetooth

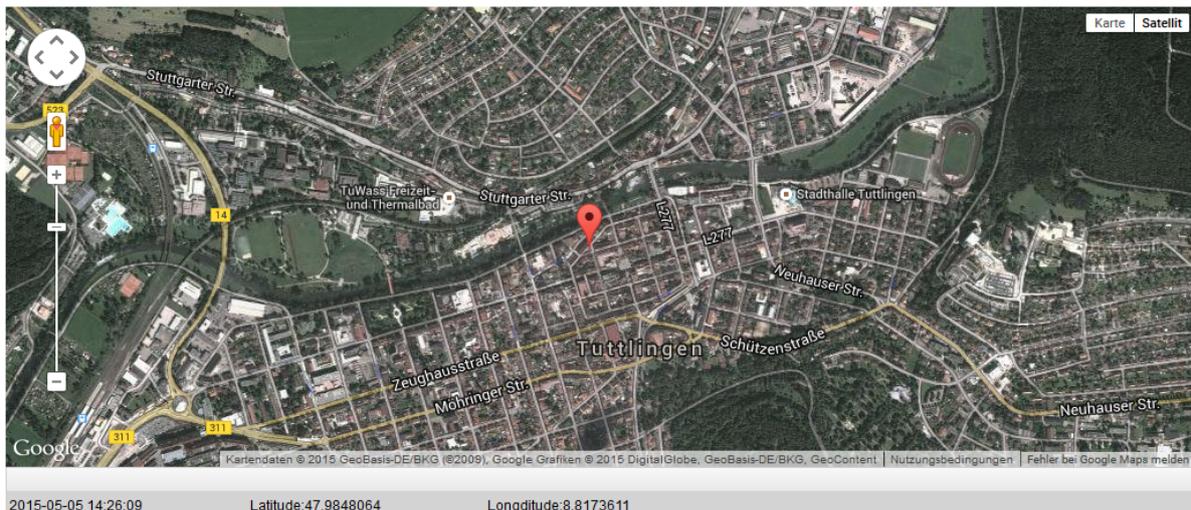
Bluetooth MAC	Bluetooth MAC Adresse
---------------	-----------------------

Security Management

Anti Theft (nur auf Device Ebene)

GPS Information (nur auf Device Ebene)

Hier können Sie den aktuellen / letzten Standort des Geräts ermitteln. Die Lokalisierung kann mit einem oder sogar zwei Passwörtern geschützt werden – Siehe: *General Settings – Privacy – GPS Access*



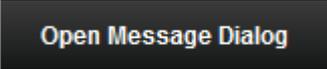
Wipe & Lock (nur auf Device Ebene)

Unter „Wipe & Lock“ können Sie folgende drei Aktionen durchführen:

Full Wipe	Das Gerät wird auf die Werkseinstellungen zurückgesetzt (sowohl geschäftliche, als auch persönliche Daten werden gelöscht)
Enterprise Wipe	Nur die Firmendaten werden vom Endgerät entfernt (Alle Apps, Daten, etc. die von AppTec übergeben wurden)
Lock Screen	Bildschirm Sperre wird aktiviert, es ist ausreichend das Gerät mit dem Geräte-Passwort/PIN wieder zu entsperren

Message (nur auf Device Ebene)

Mit „Open Message Dialog“ können Sie eine Push-Nachricht versenden.



Anschließend sollte sich folgendes Fenster öffnen, dies können Sie mit einem Subject (Betreff) und einer Message (Nachricht) füllen und an das ausgewählte Endgerät versenden.

Send a message
✕

Subject	Test: Bitte bei Ihrer IT melden
Message	<div style="border: 1px solid #add8e6; padding: 5px; margin: 5px;"> Diese Nachricht dient zur Testzwecken! Bitte melden Sie sich bei Ihrer EDV Abteilung. Mit freundlichen Grüßen Ihre IT-Abteilung </div>

Send Message

Security Configuration

Passcode

Unter „Passcode“ können Sie ein Gerätepasswort erzwingen, folgende Einstellungsmöglichkeiten stehen hier zur Verfügung

Minimum password length	Legt fest, aus wie vielen Zeichen das Passwort mindestens bestehen muss
Password quality	<p>Passwortstärke</p> <p>Unspecified = nicht spezifiziert</p> <p>Every password is ok = jedes Passwort ist zulässig</p> <p>at least numeric characters = Mindestens Zahlen müssen enthalten sein</p> <p>at least complex characters = Mindestens komplexe (Sonderzeichen) müssen enthalten sein</p> <p>at least alphanumerical characters = mindestens alphanumerische Zeichen müssen enthalten sein</p> <p>at least alphabetic characters = mindestens alphabetische Zeichen müssen enthalten sein</p>
Maximum inactivity time lock	Zeit der automatischen Tastensperre bei Inaktivität des Users
Minimum lowercase letters required in password	Mindestanzahl von kleingeschriebenen Buchstaben
Minimum uppercase letters required in password	Mindestanzahl von großgeschriebenen Buchstaben
Minimum non-letter characters required in password	Mindestanzahl wie viel "nicht-Buchstaben" Zeichen enthalten sein müssen
Minimum numerical digits required in password	Mindestanzahl wie viel Zahlen für das Passwort erforderlich sind
Minimum symbols required in password	Mindestanzahl wie viel Sonderzeichen enthalten sein müssen
Password expiration timeout	Legt fest, nach welchem Zeitraum das Passwort abläuft und ein neues Passwort vergeben werden muss
Password history restriction	Anzahl der wie viel zuletzt benutzten Passwörter nicht erlaubt sind
Maximum failed password attempts	Legt fest, wie oft das Passwort falsch eingegeben werden darf, bis ein vollständiger Wipe des Gerätes durchgeführt wird

Encryption

Unter diesem Punkt sind Sie in der Lage sowohl den internen Gerätespeicher, als auch den externen SD Kartenspeicher zu verschlüsseln.

<p>Require Storage Encryption</p>	<p>Falls diese Einstellung aktiviert wird, ist der Gerätespeicher verschlüsselt, sofern das Gerät diese Funktionalität unterstützt. Sobald der Gerätespeicher einmalig verschlüsselt wird, ist es nicht mehr möglich diesen wieder zu entschlüsseln. Ebenfalls wird die Passwort Policy automatisch auf mindestens 6 alphanumerische Zeichen umgestellt</p>
<p>Require SD Card Encryption</p>	<p>Diese Einstellung gilt nur für Samsung Geräte! Falls diese Einstellung aktiviert wird, ist die externe SD Karte verschlüsselt und kann nur manuell auf dem Endgerät unter den Einstellungen wieder entschlüsselt werden. Ebenfalls wird dann die Passwort Policy automatisch auf mindestens 6 alphanumerische Zeichen umgestellt</p>

AntiVirus

AppTec stellt kostenlos eine Antiviren App namens „IKARUS Mobile Security“ zur Verfügung, sie können folgende Dinge konfigurieren

Scan Method	Quick = Nur Apps werden auf Schadcode / Viren untersucht Full = Das komplette System wird auf Schadcode / Viren untersucht
Scan Interval	Zeitraum in welchem Intervall eine Untersuchung (Quick / Full) durchgeführt werden soll
Update Check	Wie oft ein Update der App und deren Datenbank (Viren / Schadcode) durchgeführt werden soll
Protection Mode	Es wird die App beim Starten und Installieren auf Schadcode überprüft
Self Configuration	Falls aktiv, darf der User die Einstellungen selbst am Endgerät vornehmen bzw. abändern
Connect During Roaming	Verbindungsaufbau während sich das Endgerät sich im Roaming befindet

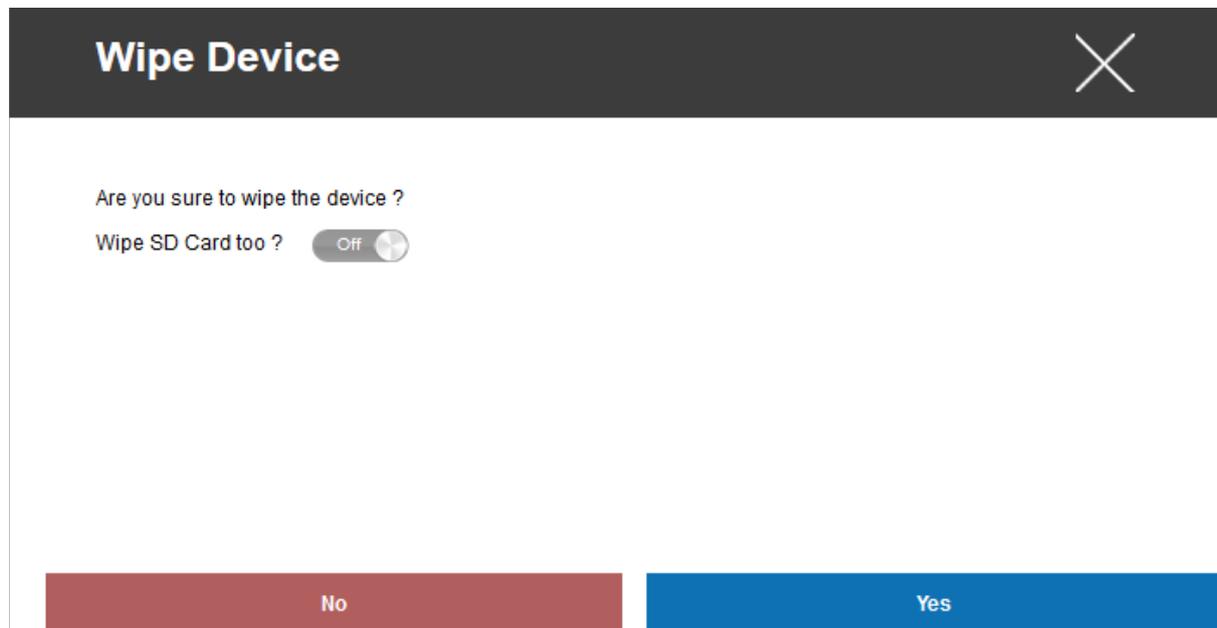
End of Life (nur auf Device Ebene)

Wipe (nur auf Device Ebene)

Unter „Wipe“ können Sie das Gerät auf die Werkseinstellungen zurücksetzen, hier werden sowohl die geschäftlichen, als auch die privaten Daten auf dem Endgerät gelöscht

Mit dem Klick auf das „Minussymbol“  sollten Sie folgende Meldung erhalten

Wipe SD Card too ?	Ebenfalls der SD-Karten Speicher wird gelöscht
--------------------	--



Mit „Yes“ können Sie die *Löschung durchführen*.

Unter „Wipe Report“ können Sie sich folgende Dinge anzeigen lassen

Wiped by	Historie von wem der Wipe ausgeführt wurde
Date	Datum
Status	Status (z.B. ob der Wipe erfolgreich durchgeführt wurde)

Restriction Settings

Restrictions

Hier können diverse Dinge unterbunden und verhindert werden.

Enable Camera	Erlaubung der Kamera
Force Auto Sync	Betrifft die Schnelleinstellung „Sync“  On = Synchronisation ist permanent aktiviert Off = Synchronisation ist permanent deaktiviert User choice = Vom User selbst wählbar
Force Bluetooth	On = Bluetooth ist permanent aktiviert Off = Bluetooth ist permanent deaktiviert User choice = Vom User selbst wählbar
Force GPS	On = GPS ist permanent aktiviert Off = GPS ist permanent deaktiviert User choice = Vom User selbst wählbar
Force Network Location	On = Permanente Internet-Lokalisierung Off = Permanente Deaktivierung der Internet-Lokalisierung User choice = Vom User selbst wählbar

Für Samsung Geräte mit der SAFE 2.0 oder höher Schnittstelle sind zusätzlich folgende Einstellungsmöglichkeiten verfügbar.

Allow SD Card	Erlauben einer SD Karte
Allow SD Card Write	Erlauben das „Schreiben“ auf der SD Karte
Allow Screen Capture	Erlauben von Screenshots
Allow Clipboard	Erlauben der Zwischenablage
Backup settings and app data in Google Cloud	Off = Google Backup deaktivieren On = Google Backup aktivieren User Choice = Userentscheidung
Allow USB Debugging	Erlauben des USB Debugging (wird z.B. benötigt um Geräte-Logs (ADB) zu erstellen)
Allow Google Crash Report	Erlaubt es dem User Fehlerberichte von Apps an Google zu schicken
Allow Factory Reset	Erlaubt es dem User manuell das Gerät auf die Werkseinstellungen zurückzusetzen
Allow OTA Upgrade	Erlauben von „Over-The-Air“ Updates
Allow USB host storage	Wenn aktiviert, kann ein externer USB Speicher in Form von einer HD oder einem SD Kartenleser angebunden werden
Allow USB Media Player (MTP,PTP)	Erlauben von USB Media Player (MTP,PTP)
Allow Microphone	On = Mikrophon für 3rd Party Apps erlauben Off = Mikrophon für 3rd Party Apps ist nicht erlaubt User Choice = Die Entscheidung des jeweiligen Users, ob die 3rd Party App auf das Mikrophon zugreifen darf
Allow NFC (Near Field Communication)	Erlauben von NFC

BYOD Container

Activation

Unter dieser Einstellung können Sie einen PIM (Personal Information Manager) Container zur Verfügung stellen.

Sie können entweder den „Google Divide“ Container oder den „SecurePIM“ Container, sowie Samsung KNOX mit den On/Off Buttons freischalten.

Die jeweilig ausgewählte App wird dann automatisch auf dem Endgerät installiert.

Knox Passcode

Legen Sie Richtlinien fest, welche die Einstellungen für das Gerätepasswort betreffen

Minimum password length	Legt fest, aus wie vielen Zeichen das Passwort mindestens bestehen muss
Password quality	<p>Passwortstärke</p> <p>Every password is ok = jedes Passwort ist zulässig</p> <p>At least numeric characters = Mindestens Zahlen müssen enthalten sein</p> <p>At least complex characters = Mindestens komplexe (Sonder-) Zeichen müssen enthalten sein</p> <p>At least alphanumerical characters = mindestens alphanumerische Zeichen müssen enthalten sein</p> <p>At least alphabetic characters = mindestens alphabetische Zeichen müssen enthalten sein</p>
Minimum compley characters required	Mindestanzahl von komplexen Buchstaben
Maximum Inactivity Timeout	Zeit der automatischen Tastensperre bei Inaktivität des Users
Allow Fingerprint Authentication	Erlauben des Entsperrens via Fingerabdruck
Allow Iris Authentication	Erlauben des Entsperrens via Augenerkennung
Max Password Age	Legt fest, nach welchem Zeitraum das Passwort abläuft und ein neues Passwort vergeben werden muss
Stored Password History	Anzahl der wie viel zuletzt benutzten Passwörter nicht erlaubt sind
Maximum failed password attempts	Legt fest, wie oft das Passwort falsch eingegeben werden darf, bis ein vollständiger Wipe des Gerätes durchgeführt wird

Knox Security

Schränken Sie bestimmte Funktionalitäten des Gerätes ein

Enable Camera	Lasse das Benutzen der Kamera zu
Allow Samsung KNOX App Store	Erlaube die Benutzung des KNOX App Stores
Allow Google Play Services	Erlaube die Benutzung der Google Play Dienste
Allow Browser	Erlaube die Benutzung des nativen Browsers
Allow Screenshots	Erlaube das Erstellen von Bildschirmfotos
Allow Contact Import	Wenn aktiviert, so kann im KNOX Container auf die Gerätekontakte zugegriffen werden
Allow Contact Export	Wenn aktiviert, so kann vom Gerät aus auf die KNOX Kontakte zugegriffen werden
Allow Calendar Import	Wenn aktiviert, so kann im KNOX Container auf den Gerätekalender zugegriffen werden
Allow Calendar Export	Wenn aktiviert, so kann vom Gerät aus auf den KNOX Kalender zugegriffen werden
Allow Non-Secure Keypad	Lasse das Benutzen einer nicht sicheren Tastatur zu
Enable File Import	Aktivieren Sie den Dateiimport in den KNOX Container
Enable File Export	Aktivieren Sie den Datelexport aus dem KNOX Container

Knox Exchange

Hier können Sie ein Exchange-Profil für den KNOX Container konfigurieren.

eMail Address	Die Mitgegebene E-Mail Adresse des jeweiligen Users Beachten Sie hier die „Placeholders“, anhand von diesen können Sie mit Credentials arbeiten und müssen nicht für jedes Gerät eine händische Änderung vornehmen Mit einem Klick auf  können Sie sich diese anzeigen lassen
Server Hostname	Serveradresse Ihres Exchange Servers
Login name	Der Login-Name für das jeweilige Endgerät, beachten Sie hier ebenfalls die „Placeholders
Domain	Domain Adresse
Password (nur auf Device Ebene)	Optional kann direkt für ein einzelnes Gerät ein Passwort mitgegeben werden, sollte dies leer gelassen werden, wird der User aufgefordert sein Exchange Passwort einzugeben
Number of previous days to sync	Zeitraum wie viel Mails zurück-synchronisiert werden sollen
Signature	Es kann eine Signatur mitgegeben werden
Default Account	Legt fest, dass dieses Mailkonto das Standard Konto ist
Use Secure Sockets Layer (SSL)	Benutzung einer SSL Verbindung
Use Transport Layer Security (TLS)	Benutzung einer TLS Verbindung
Accept all certificates	Alle Zertifikate werden akzeptiert, bitte wählen Sie diese Option aus, falls Ihr Exchange Server self-signed Zertifikate nutzt

Knox eMail

eMail Address	Die mitgegebene E-Mail Adresse des jeweiligen Users Beachten Sie hier die „Placeholders“, anhand von diesen können Sie mit Credentials arbeiten und müssen nicht für jedes Gerät eine händische Änderung vornehmen Mit einem Klick auf 
---------------	--

	können Sie sich diese anzeigen lassen
Incoming server protocol	Eingehendes Server Protokoll → IMAP oder POP
Incoming server address	Eingehende Serveradresse
Incoming server port	Eingehender Serverport
Incoming server login/username	Eingehender Server Login / Benutzername
Incoming server password	Eingehendes Serverpasswort
Incoming server uses SSL	Eingehender Server benutzt SSL
Incoming server uses TLS	Eingehender Server benutzt TLS
Incoming server accept all certificates	Eingehender Server akzeptiert jegliche Art von Zertifiakten
Outgoing server protocol	Ausgehendes Server Protokoll → SMTP
Outgoing server port	Ausgehender Serverport
Outgoing Server uses extra credentials	Zusätzliche Daten für den ausgehenden Server, wenn dies auf "off" steht, werden die eingehenden Server Einstellungen verwendet
Outgoing server login/username	Ausgehender Server Login / Benutzername
Outgoing server password	Ausgehendes Serverpasswort
Outgoing server uses SSL	Ausgehender Server benutzt SSL
Outgoing server uses TLS	Ausgehender Server benutzt TLS
Outgoing server accept all certifiactes	Ausgehender Server akzeptiert jegliche Art von Zertifikaten
Signature	Hierüber kann eine Signatur mitgegeben warden
Notify user on receiving new eMail	User wird bei einer neuen Mail benachrichtigt

Knox Apps

Legen Sie hier Apps fest, welche Sie an die Engeräte verteilen wollen. Diese werden daraufhin im KNOX-Container zur Verfügung stehen. Um eine App hinzuzufügen, gehen Sie bitte vor wie im Menüpunkt Mandatory Apps

Application Name	Name der Applikation
Mandatory Since	Zeitpunkt, wann die App hinzugefügt wurde
Source	Quelle der App (Play Store In-House)

Durch Klicken des  Symbols kann die entsprechende App wieder entfernt werden

Connection Management

Wifi

Nehmen Sie an dieser Einstellung die Vorkonfiguration der Endgeräte für den Zugriff auf interne Access Points vor

Services Set Identifier (SSID)	SSID des zu verbindenden Netzwerks
Hidden Network	Aktivieren, falls der AP die SSID nicht broadcastet
Security Type	Sicherheitstyp des AP festlegen
WEP	
Password	Passwort für den AP
WPA/WPA2	
Password	Passwort für den AP
802.1x EAP	
EAP-Method	
PWD	Aktivieren bzw. Deaktivieren
PEAP	Aktivieren bzw. Deaktivieren
TTLS	Aktivieren bzw. Deaktivieren
TLS	Aktivieren bzw. Deaktivieren
Authentication	
PWD	
Identity	Identität
Password	Passwort
PEAP	
Phase 2 Authentication Protocol	Protokoll der 2nd Authentifizierung
none	Kein weiteres Protokoll
MSCHAPV2	MSCHAPV2 Protokoll
GTC	GTC Protokoll
CA Certificate	CA Zertifikat
Identity	Identität
Anonymous Identity	Anonyme Identität
Password	Passwort
TTLS	
Phase 2 Authentication Protocol	Protokoll der 2nd Authentifizierung
none	Kein weiteres Protokoll
PAP	PAP Protokoll
MSCHAP	MSCHAP Protokoll
MSCHAPV2	MSCHAPV2 Protokoll
GTC	GTC Protokoll
CA Certificate	CA Zertifikat
Identity	Identität
Anonymous Identity	Anonyme Identität

Password	Passwort
TLS	
CA Certificate	CA Zertifikat
Identity	Identität
Password	Passwort

VPN

Connection Type	VPN-Verbindungstyp festlegen
Cisco AnyConnect	
Connection Name	Verbindungsname der VPN
Server	Serveradresse
Certificate Mode	Disabled = deaktiviert Automatic = automatisch
L2TP (SAFE 2.x)	Nur für SAFE 2.x Geräte verfügbar
Connection Name	Verbindungsname
Server	Serveradresse
Enable L2TP Secret	
DNS Search Domains	DNS Suchdomainen
PPTP (SAFE 2.0+)	Nur für SAFE 2.0 oder höher verfügbar
Connection Name	Verbindungsname der VPN
Server	Serveradresse
Enable Encryption	Verschlüsselung aktivieren
DNS Search Domains	DNS Suchdomainen
L2TP / IPSec PSK (SAFE 2.0+)	Nur für SAFE 2.0 oder höher verfügbar
Connection Name	Verbindungsname der VPN
Server	Serveradresse
IPSec Pre-Shared Key	Pre-Shared Key zur Authentifizierung
Enable L2TP Secret	
L2TP Secret	
DNS Search Domains	DNS Suchdomainen
IPSec XAuth PSK (SAFE 3.0+)	Nur für SAFE 3.0 oder höher verfügbar
Connection Name	Verbindungsname der VPN
Server	Serveradresse
IPSec Identifier	Benutzername für die Verbindung
IPSec Pre-Shared Key	Passwort für die Verbindung
DNS Search Domains	DNS Suchdomainen
OpenVPN	
Connection Name	Verbindungsname
OpenVPN Profile	Hier wird der Inhalt der .ovpn Datei hineinkopiert
OpenVPN App	Es gibt zwei unterschiedliche Apps für die Nutzung von OpenVPN Wir empfehlen die „OpenVPN for Android“ App, alternativ kann aber auch die „OpenVPN Connect“ App genutzt werden

Restrictions

Hier können Sie diverse Restriktionen einstellen in der Hinsicht auf das Verbindungs-Management.

Allow Data Roaming	Das Erlauben von mobilen Daten im Roaming
Force Data Roaming	Falls aktiviert, ist Roaming für mobile Daten permanent aktiviert (nicht empfehlenswert!) Diese Einstellung überschreibt die „Allow Data Roaming“ einstellung!
Folgende Einstellung sind nur für SAFE 2.0 Geräte oder ggfs. höher verfügbar	
Allow Emergency Calls Only	Es können nur Notrufe getätigt werden
Allow WiFi	Erlauben von WiFi
WiFi Netwok Minimum Security Level	Mindestanforderung des Sicherheitslevels einer WiFi Verbindung Open = alle WiFi Typen sind zulässig
Forbid user to add WiFi networks	Der User darf selbst keine WiFi Netzwerke hinzufügen Diese Einstellung ist nur dann möglich, wenn ein WiFi Profil unter dem „Connection Management“ definiert wurde
Allow SMS & MMS	All = Alles an SMS & MMS Verkehr ist erlaubt Incoming SMS Only = Nur eingehende SMS Nachrichten sind erlaubt Outgoing SMS Only = Nur ausgehende SMS Nachrichten sind erlaubt None = Kein SMS / MMS Verkehr ist zulässig
Allow Sync during Romaing	Erlauben einer Synchronisation während das Gerät sich im Roaming befindet On = aktiviert Off = deaktiviert User choice = Entscheidung des Users
Allow Voice Roaming	Erlauben des Sprach-Roamings On = aktiviert Off = deaktiviert User Choice = Entscheidung des Users

APN

Folgende Einstellungen sind nur für Samsung SAFE 2.0 oder ggf. höher verfügbar!	
APN Display Name	Anzeigender APN Name
Access Point Name	Name des APNs
Outgoing server protocol	
Not set	
None	
PAP	PAP Protokoll
CHAP	CHAP Protokoll
PAP or CHAP	Entweder das PAP oder CHAP Protokoll
MCC – Mobile Country Code	Hier wird der MCC eingetragen, lassen Sie dieses Feld leer falls der MCC der eingelegten SIM-Karte genutzt werden soll
MNC – Mobile Network Code	Hier wird der MNC eingetragen, lassen Sie dieses Feld leer falls der MNC der eingelegten SIM-Karte genutzt werden soll
Server address	Serveradresse
Server port number	Serverportnummer
Server proxy address	Serveradresse des Proxys
MMS server address	MMS Serveradresse, für Standard bitte freilassen
MMS prt number	MMS Portnummer
MMS proxy address	MMS Proxy Adresse
User name	Username
Password	Passwort
Access Point Type	Erlaubte Typen sind „default“, „mms“, „supl“ Falls dieses Feld leer gelassen wird, wird „default,supl,mms“ genutzt
Preferred APN	APN wird bevorzugt

Bluetooth

Hier können diverse Bluetooth Einstellung vorgenommen werden

Folgende Einstellungen sind nur für Samsung SAFE 2.0 oder höher verfügbar!	
Allow Device discovery via Bluetooth	Erlauben ob das Gerät hinsichtlich Bluetooth sichtbar ist
Allow Bluetooth Pairing	Erlaubt dem Gerät das Koppeln von Bluetooth Geräten
Allow Bluetooth Headset devices	Erlauben von Bluetooth Headsets
Allow Bluetooth Hands-free devices	Erlauben von Freisprech-Bluetooth Geräten
Allow Bluetooth A2DP devices	Erlauben des Audio Streamings Protokolls A2DP zwischen Geräten
Allow Outgoing Calls	Erlaubt ausgehende Anrufe über BT
Allow Data Transfer via Bluetooth	Erlaubt den Datenaustausch mithilfe von Bluetooth
Allow Bluetooth Tethering	Erlaubt die Nutzung des Gerät als Modem (Bluetooth Internetverbindung)
Allow connection to Computer via Bluetooth	Erlaubt es dem Gerät sich mit einem Computer über Bluetooth zu verbinden

PIM Management

Exchange

Nur für Samsung SAFE 1.0 oder höher verfügbar!	
eMail Address	<p>Die Mitgegebene E-Mail Adresse des jeweiligen Users Beachten Sie hier die „Placeholders“, anhand von diesen können Sie mit Credentials arbeiten und müssen nicht für jedes Gerät eine händische Änderung vornehmen</p> <p>Mit einem Klick auf  können Sie sich diese anzeigen lassen</p>
Server Hostname	Serveradresse Ihres Exchange Servers
Login name	Der Login-Name für das jeweilige Endgerät, beachten Sie hier ebenfalls die „Placeholders
Password (nur auf Device Ebene)	Optional kann direkt für ein einzelnes Gerät ein Passwort mitgegeben werden, sollte dies leer gelassen werden, wird der User aufgefordert sein Exchange Passwort einzugeben
Domain	Domain Adresse
Number of previous days to sync	Zeitraum wie viel Mails zurück-synchronisiert werden sollen
Signature	Es kann eine Signatur mitgegeben werden
Default Account	Legt fest dass dieses Mailkonto das Standard Konto ist
Use Secure Sockets Layer (SSL)	Benutzung einer SSL Verbindung
Use Transport Layer Security (TLS)	Benutzung einer TLS Verbindung
Accept all certificates	Alle Zertifikate werden akzeptiert, bitte wählen Sie diese Option aus, falls Ihr Exchange Server self-signed Zertifikate nutzt

eMail

Hier können Sie IMAP und POP Konten an die jeweiligen Endgeräte verteilen.

Diese Einstellung ist nur für Samsung SAFE 2.0 oder höher verfügbar!	
eMail Address	<p>Die mitgegebene E-Mail Adresse des jeweiligen Users Beachten Sie hier die „Placeholders“, anhand von diesen können Sie mit Credentials arbeiten und müssen nicht für jedes Gerät eine händische Änderung vornehmen</p> <p>Mit einem Klick auf  können Sie sich diese anzeigen lassen</p>
Incoming server protocol	Eingehendes Server Protokoll → IMAP oder POP
Incoming server address	Eingehende Serveradresse
Incoming server port	Eingehender Serverport
Incoming server login/username	Eingehender Server Login / Benutzername
Incoming server password (nur auf Device Ebene)	Eingehendes Serverpasswort
Incoming server uses SSL	Eingehender Server benutzt SSL
Incoming server uses TLS	Eingehender Server benutzt TLS
Incoming server accept all certificates	Eingehender Server akzeptiert jegliche Art von Zertifikaten
Outgoing server protocol	Ausgehendes Server Protokoll → SMTP
Outgoing server port	Ausgehender Serverport
Outgoing Server uses extra credentials	Zusätzliche Daten für den ausgehenden Server, wenn dies auf “off“ steht, werden die eingehenden Server Einstellungen verwendet
Outgoing server login/username	Ausgehender Server Login / Benutzername
Outgoing server password (nur auf Device Ebene)	Ausgehendes Serverpasswort
Outgoing server uses SSL	Ausgehender Server benutzt SSL
Outgoing server uses TLS	Ausgehender Server benutzt TLS
Outgoing server accept all certificates	Ausgehender Server akzeptiert jegliche Art von Zertifikaten
Signature	Hierüber kann eine Signatur mitgegeben werden
Notify user on receiving new eMail	User wird bei einer neuen Mail benachrichtigt

Touchdown Exchange

Sollten Sie Touchdown (3rd Party App) benutzen wollen, können Sie dies hier freischalten und im Vorfeld konfigurieren.

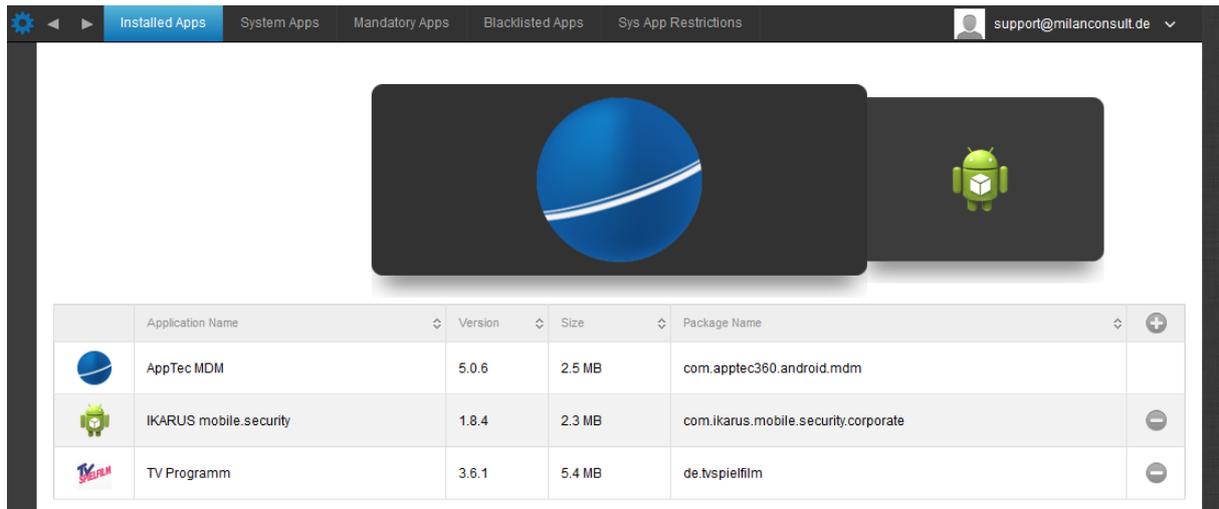
Hostname of the Exchange Server	Hostname Ihres Exchange Servers (FQDN oder IP Adresse)
eMail Address for the Exchange Account	Die Mitgegebene E-Mail Adresse des jeweiligen Users Beachten Sie hier die „Placeholders“, anhand von diesen können Sie mit Credentials arbeiten und müssen nicht für jedes Gerät eine händische Änderung vornehmen Mit einem Klick auf  können Sie sich diese anzeigen lassen
Username for the Exchange Account	Der Username für das jeweilige Endgerät, beachten Sie hier ebenfalls die „Placeholders“
Password for the Exchange Account (nur auf Device Ebene)	Optional kann direkt für ein einzelnes Gerät ein Passwort mitgegeben werden, sollte dies leer gelassen werden, wird der User aufgefordert sein Exchange Passwort einzugeben
Allow User to Change Email Signature	Dem User erlauben, dass er seine Signatur ändern darf
License Key	Touchdown muss separat lizenziert werden, hier muss Ihr Lizenz-Code eingetragen werden
Device Type reported in Exchange Server	Legen Sie hier die Bezeichnung fest, die vom Gerät an den Exchange Server mitgeteilt werden soll
Allow Backup if Emails and Settings	Erlauben eines Backups von Emails und Einstellungen
Allow Self signed certificates	Erlauben von selbst-signierten Zertifikaten
Allow HTML Formatted Email	Erlauben von HTML formatierten E-Mails
Allow Attachments	Nutzung von Anhängen erlauben
Enable TouchDown Widgets	Sollte diese Einstellung aktiviert sein, kann der User die TouchDown Widgets auf seinem Endgerät nutzen
Maximum Attachment Size (KB)	Legt in KB fest, wie groß ein Anhang maximal sein darf
Maximum Email size (KB)	Legt in KB fest, wie groß eine Mail sein darf, sollte diese Grenze überschritten werden, wird diese Mail bis zur passenden Größe beschnitten
Signature	Vordefinierte Signatur

App Management

Enterprise App Manager

Installed Apps (nur auf Device Ebene)

Hier werden Ihnen alle Apps angezeigt, die aktuell auf dem jeweiligen Endgerät



	Application Name	Version	Size	Package Name	
	AppTec MDM	5.0.6	2.5 MB	com.apptec360.android.mdm	+
	IKARUS mobile.security	1.8.4	2.3 MB	com.ikarus.mobile.security.corporate	-
	TV Programm	3.6.1	5.4 MB	de.tvspielfilm	-

installiert sind.

Über das _Symbol lassen sich direkt neue Apps auf das Endgerät pushen.

Sie können sowohl eine „Google Play Store“ App aus dem öffentlich AppStore auf das Gerät pushen.

✕

Select an application

Google Play Store Android In-House Apps

German
Free Apps
Search Now

	DB Navigator Deutsche Bahn free	App Berechtigungen - Datenschutz ist uns wichtig. Für Informationen über die Berechtigungen der App DB Navigator besuchen Sie bitte: www.bahn.de/androidrechte Egal ob ICE, S-Bahn, Bus oder Straßenbahn, Sie haben stets Zugriff auf den aktuellen Fahrplan in ganz Deutschland und Europa mit über 250.000 Haltestellen. Mit Echtzeit-Informat ...
	DB Zugradar Deutsche Bahn free	Alle Züge auf einen Blick: Mit dem DB Zugradar verfolgen Sie die Züge des DB Nah- und Fernverkehrs live im DB Zugradar und grenzen Sie durch den Filter die Darstellung der Verkehrsmittel (Fernverkehr (ICE und IC/EC), Nahverkehr) und Bahnhöfe ein. Der DB Zugradar stellt auf einer dynamischen Karte das gesamte Streckennetz der Deutschen B ...
	Schallmessung : Sound Meter Smart Tools co. free	Sound Level Meter ist im Paket 4 der Smart Tools Sammlung. (Lautstärke)Achtung!! Die meisten Mikrofone sind für die menschliche Stimme (300-3400Hz, 40-60dB) ausgelegt. Also sind die maximalen Werte der Hardware begrenzt. Motorola Milestone(max. 100), Galaxy S(max. 81), Galaxy S2(98dB), Galaxy Tab und HTC Desire HD wurden mit echten Schallpe ...
	München Navigator Deutsche Bahn free	Egal ob Sie die S- oder U-Bahn, die Tram oder den Bus nutzen, mit dem München Navigator (ehemals: Navi S-Bahn München) können Sie ab sofort Ihr passendes Handy-Ticket für den gesamten Münchner Verkehrsverbund (MVG) bis kurz vor Fahrtbeginn kaufen und sich zusätzlich über die Position ihres Zuges oder eventuelle baubedingte Störungen i ...
	Öffi - Fahrplanauskunft	All-in-one App für die Öffentlichen Verkehrsmittel: • Echtzeit-Abfahrtszeiten (inkl. Verspätungen), • nahegelegene Haltestellen (mit Karte). • Verbindungs-Abfragen (von Haustür zu Haustür) und •

Oder Sie wählen unter der Kategorie „Android In-House Apps“ einer Ihrer unter den General Settings hochgeladene In-House App aus.

✕

Select an application

Google Play Store Android In-House Apps

Uploaded In-House Apps
Upload In-House App

	IBM Notes Traveler Version:9.0.1.3 201411210833-T7.1.0.0.52-271G forgepond.com.lotus.sync.traveler	No description available	
---	---	--------------------------	---

Sie können auch direkt über „Upload In-House App“ eine apk Datei auswählen und diese direkt hochladen.

Upload an In-House App ✕

Upload Limit: max. size of apk files is 64 MB
Select the .apk file of the Android application which you want to upload

Keine Datei ausgewählt.

System Apps (nur auf Device Ebene)

Unter den „System Apps“ werden Ihnen alle Apps und Dienste aufgeführt, die bereits

Installed Apps
System Apps
Mandatory Apps
Blacklisted Apps
Sys App Restrictions
support@milanconsult.de



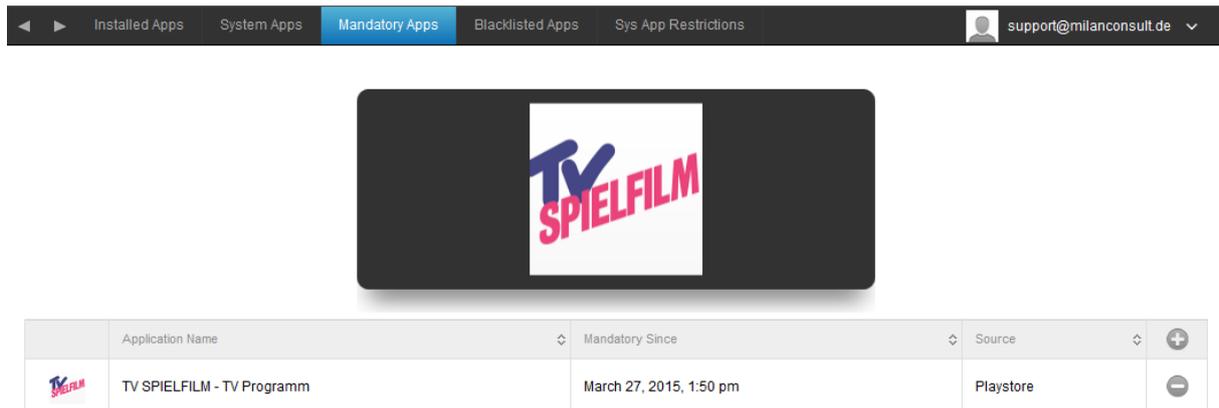
	Application Name	Version	Size	Package Name
	Adapt Sound	1.0	2.8 MB	com.sec.hearingadjust
	AllShare ControlShare Service	1.0.0	355 kB	com.sec.android.allshare.service.cont...
	AllShare FileShare Service	1.4r476	39 kB	com.sec.android.allshare.service.file...
	Android-System	4.3-I9300XXUGNG3	35 MB	android
	Application installer	1.0	39 kB	com.sec.android.preloadinstaller
	BadgeProvider	1.0	4 kB	com.sec.android.provider.badge
	BandService	1.42	518 kB	com.sec.android.band
	Basic Daydreams	4.3-I9300XXUGNG3	32 kB	com.android.dreams.basic
	Benutzerhandbuch	1.0	23 kB	com.sec.android.widgetapp.webmanual
	Best Face	20130529.1.0.0.46	199 kB	com.arcsoft.picturesbest.app
	Bevorzugte Apps	1.0	1.4 MB	com.sec.android.favoriteappwidget

von Ihrem Gerätehersteller aus auf dem Endgerät installiert sind.

Mandatory Apps

Unter den Mandatory Apps können Sie zwingend erforderliche Apps festlegen. Der User wird ständig dazu aufgefordert sich diese besagte App zu installieren. Über das  kann direkt eine zwingend erforderliche App definiert werden.

Dies kann wie bei den „Installed Apps“ eine Google Play Store App sein, aber auch eine In-House App.

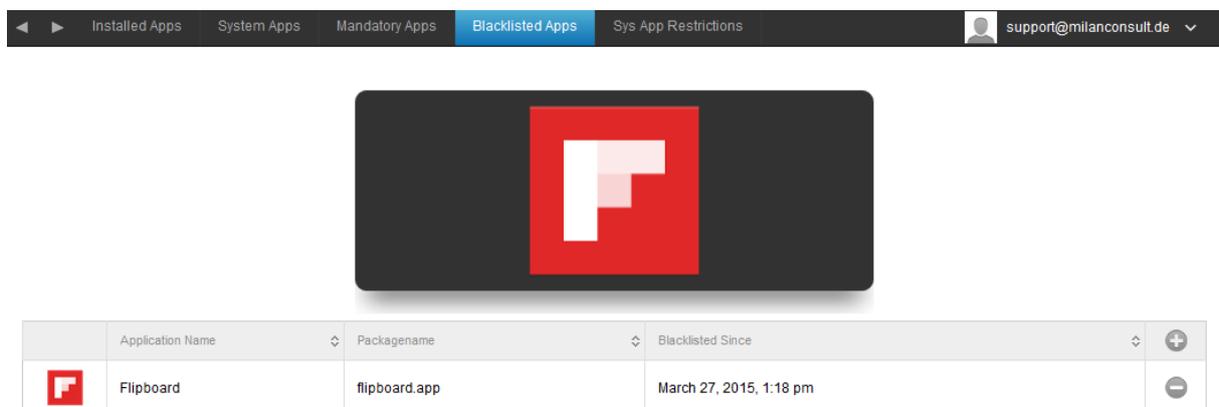


	Application Name	Mandatory Since	Source	
	TV SPIELFILM - TV Programm	March 27, 2015, 1:50 pm	Playstore	

Die Bedienung funktioniert exakt gleich wie bei der Kategorie „Installed Apps“.

Blacklisted Apps

Unter „Blacklisted Apps“ können Sie Apps oder Dienste definieren, die nicht auf dem Endgerät installiert werden können bzw. diese werden deaktiviert und für den User unausführbar gemacht.



	Application Name	Packagename	Blacklisted Since	
	Flipboard	flipboard.app	March 27, 2015, 1:18 pm	

Über das  können Sie weitere blacklisted Apps oder Dienste hinzufügen.

Sie können entweder eine Google Play Store App auswählen.

Select an application
✕

Google Play Store **Packagename**

German ▾

Free Apps ▾

Search Now

Oder einen „Packagename“ definieren.

Select an application
✕

Google Play Store **Packagename**

Add Package

Diesen Packagename finden Sie entweder unter den „Installed Apps“ / „System Apps“ unter „Package Name“ oder Sie können ihn anhand des Google Play Store Links herausfinden.

Beispiel:

App Name: TV Spielfilm – TV Programm

Google Play Store Link:

<https://play.google.com/store/apps/details?id=de.tvspielfilm&hl=de>

Der Packagename ist dann dieser ab dem „Gleichheitszeichen“ und geht bis zu dem „Und-Zeichen“.

Packagename: de.tvspielfilm

Dies ist bei allen Google Play Store Apps identisch.

Sys App Restrictions

Unter „Sys App Restrictions“ können Sie unter anderem diverse vorinstallierte Apps und Dienste nach Ihren Wünschen blockieren.

Disable Browser	Deaktivierung des Standards Browsers
Disable Calendar	Deaktivierung vom nativen Kalender
Disable Calculator	Deaktivierung des Taschenrechners
Disable Chrome Browser	Deaktivierung des Chrome Browsers
Disable Clock	Deaktivierung der Uhr
Disable Contacts	Deaktivierung der Kontakte
Disable Dialer	Deaktivierung der nativen Telefon-App
Disable eMail	Deaktivierung von E-Mails
Disable Exchange	Deaktivierung von Exchange Konten
Disable Facebook	Deaktivierung der Facebook App
Disable Gallery	Deaktivierung der nativen Galerie-App
Disable Gmail	Deaktivierung von GMail
Disable Google Books	Deaktivierung von Google Books
Disable Google Play Kiosk	Deaktivierung von Google Play Kiosk
Disable Google Maps	Deaktivierung von Google Maps
Disable Google Music	Deaktivierung von Google Musik
Disable Google Movies	Deaktivierung von Google Movies
Disable Google Play Store	Deaktivierung des Google Play Stores (öffentlich App Store)
Disable Google Plus	Deaktivierung von Goolge Plus
Disable Google Search	Deaktivierung von der Google Suche
Disable Googkle Talk / Google Hangouts	Deaktivierung von Google Talk bzw. Google Hangouts
Disable Music Player	Deaktivierung der nativen Musik App
Disable Settings	Deaktivierung der Geräte-Einstellungen
Disable Sim Toolkit	Deaktivierung des Sim Toolkit Dienstes
Disable SMS / MMS	Deaktivierung von SMS und MMS
Disable Street View	Deaktivierung der Street View Dienste
Disable Youtube	Deaktivierung von YouTube

Samsung Apps

Unter „Samsung Apps“ können Sie für Samsung Geräte noch folgende, zusätzliche Einstellungen bzw. Restriktionen definieren.

Disable AllShare Play / Samsung Link	Deaktivierung von AllShare Play / Samsung Link
Disable ChatON	Deaktivierung von ChatON
Disable Game Hub	Deaktivierung von Game Hub
Disable Group Play	Deaktivierung von Group Play
Disable Help	Deaktivierung der Samsung Hilfe
Disable KNOX	Deaktivierung des Samsung KNOX Containers
Disable Memo	Deaktivierung von Sprachmemos
Disable My Files	Deaktivierung von „Eigene Dateien“
Disable Optical Reader	Deaktivierung des Bild-Scanners
Disable Polaris Office	Deaktivierung von Polaris Office
Disable Readers Hub / Samsung Books	Deaktivierung von Readers Hub bzw. Samsung Books
Disable S Memo	Deaktivierung der Notiz-App von Samsung
Disalbe S Translator	Deaktivierung der Übersetzer App von Samsung
Disable S Voice	Deaktivierung des Sprachassistenten S Voice
Disable Samsung Apps	Deaktivierung des Samsung App Stores
Disable Samsung Hub	Deaktivierung des Entertainment Stores von Samsung
Disalbe Video Player	Deaktivierung des Video Players
Disable Voice Recorder	Deaktivierung der Sprachaufnahme
Disable WatchON	Deaktivierung von WatchON (simuliert eine Fernbedienung)

Huawei Apps

Unter „Huawei Apps“ können Sie für Huawei Geräte noch folgende, zusätzliche Einstellungen bzw. Restriktionen definieren.

Disable DLNA	Deaktivierung von DLNA
Disable App Installer	Deaktivierung des App Installers
Disable File Manager	Deaktivierung des Datei Managers
Disable Backup Manager	Deaktivierung des Backup Managers
Disable System Updater	Deaktivierung des System Updaters
Disable Tool Box	Deaktivierung der Tool Box
Disable Weather	Deaktivierung des Wetterdienstes
Disable FM Radio	Deaktivierung von FM Radio

Enterprise App Store

Playstore

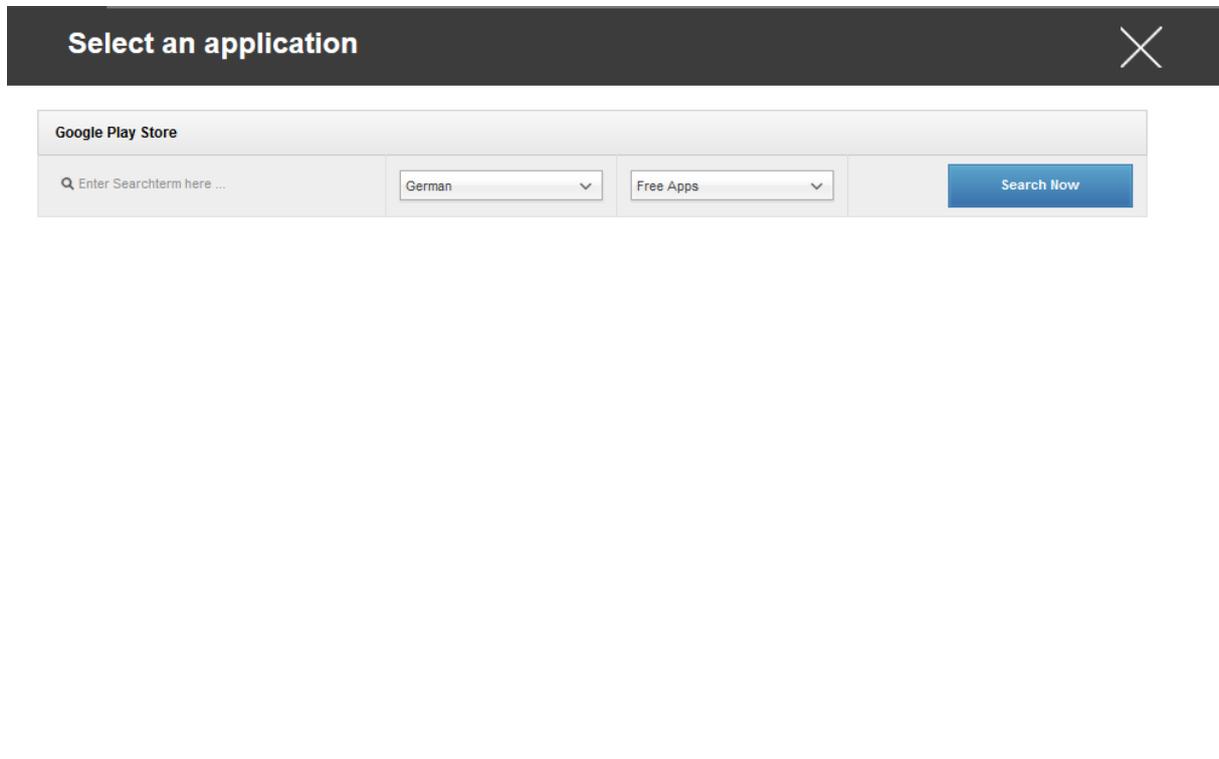
Unter diesem Punkt können Sie optionale Apps für Ihre User verteilen.

Dies sind lediglich Verlinkungen auf den offiziellen Google Play Store, aus diesem Grund muss auf jedem Endgerät eine Google ID hinterlegt sein. Wir empfehlen an dieser Stelle, dass jeder User seine eigene Google Play Store ID besitzt.

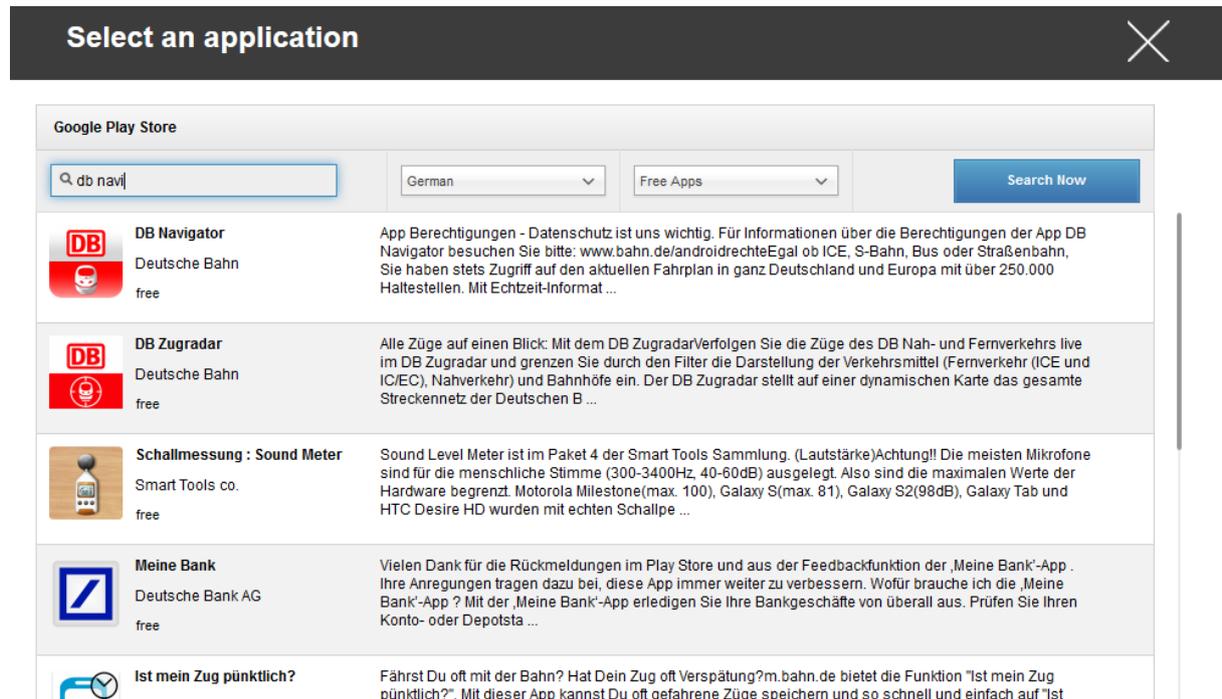
Mit dem  können Sie weitere Apps hinzufügen.



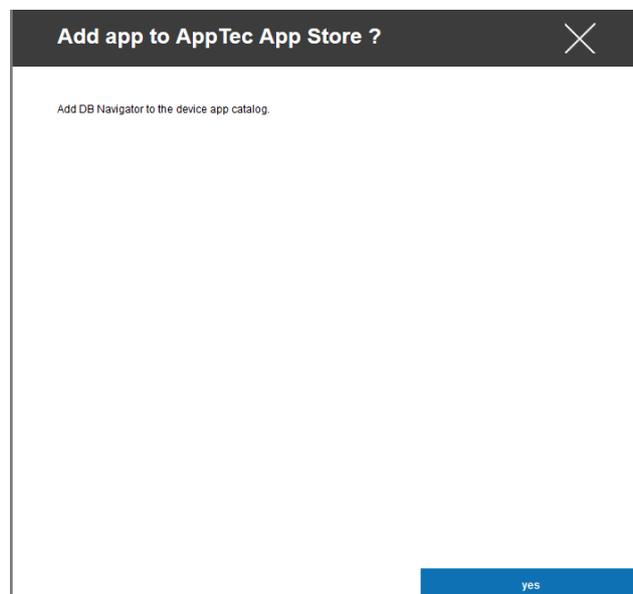
Danach sollte sich ein Fenster mit folgender Übersicht öffnen.



Bei „Enter Searchterm here ...“ können Sie nach einer sich im Google Play Store befindenden App suchen.



Wenn Sie nun auf das Icon oder auf den Name der App klicken, werden Sie nochmals gefragt, ob Sie diese App dem App Katalog hinzufügen möchten – bestätigen Sie dies mit „yes“.



Sollte der App-Store Import erfolgreich gewesen sein, erhalten Sie nun folgende Übersicht:



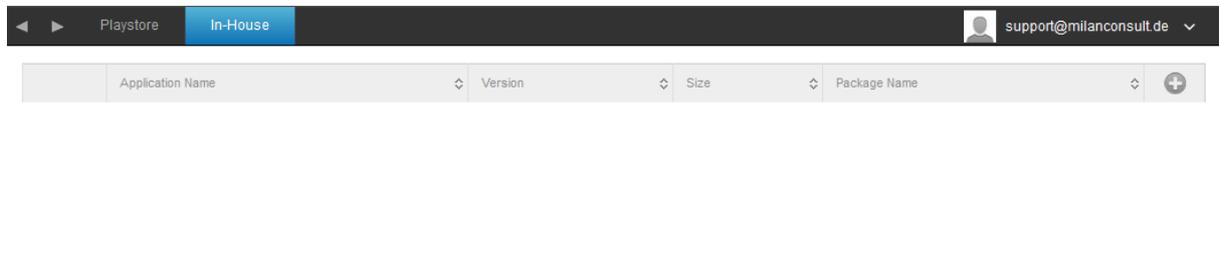
Somit ist der App-Store Import abgeschlossen und der User kann nun auf dem Endgerät den AppStore von AppTec sehen.

Wenn der User diesen Store öffnet, kann er ihm alle zugewiesenen Apps sehen und installieren.

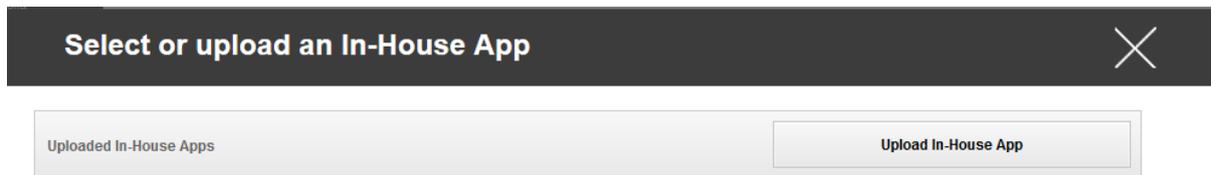
In-House

Unter dem Punkt „In-House“ können Sie Ihre eigenentwickelten Apps hochladen und verteilen.

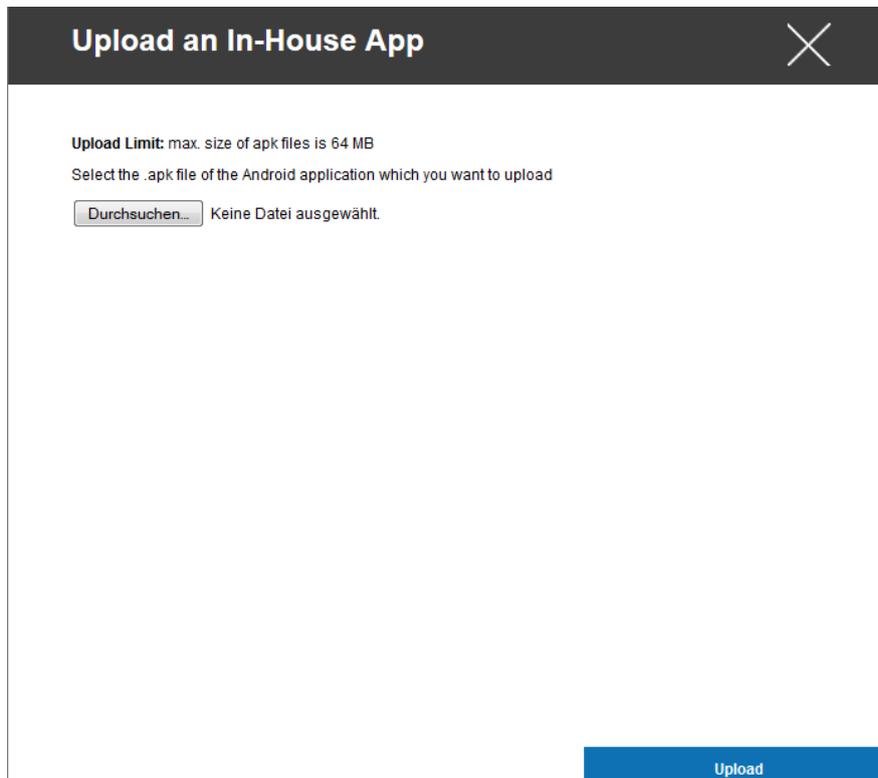
Mit dem  können Sie weitere In-House Apps verteilen.



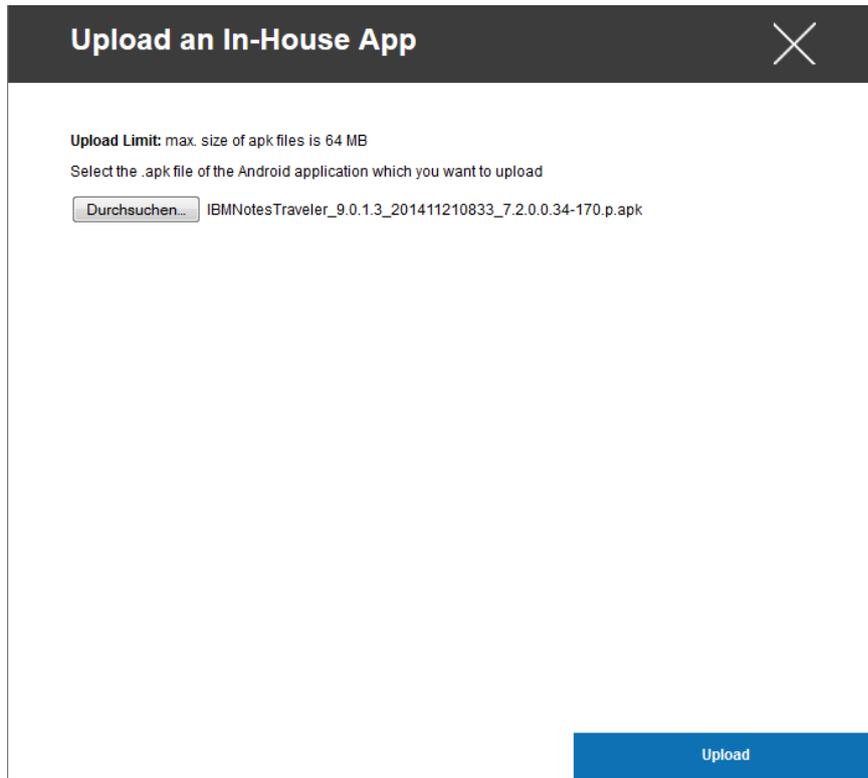
Sollten Sie bisher noch keine In-House App verteilt haben, erhalten Sie nun folgende Übersicht:



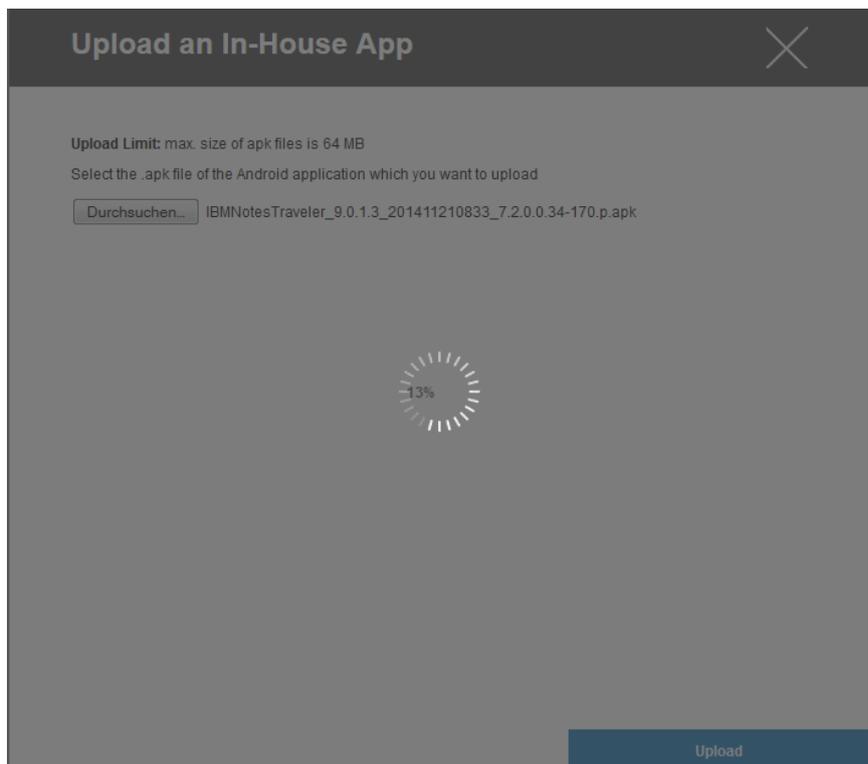
Klicken Sie hierzu auf “Upload In-House App”, nun erhalten Sie folgende Ansicht:



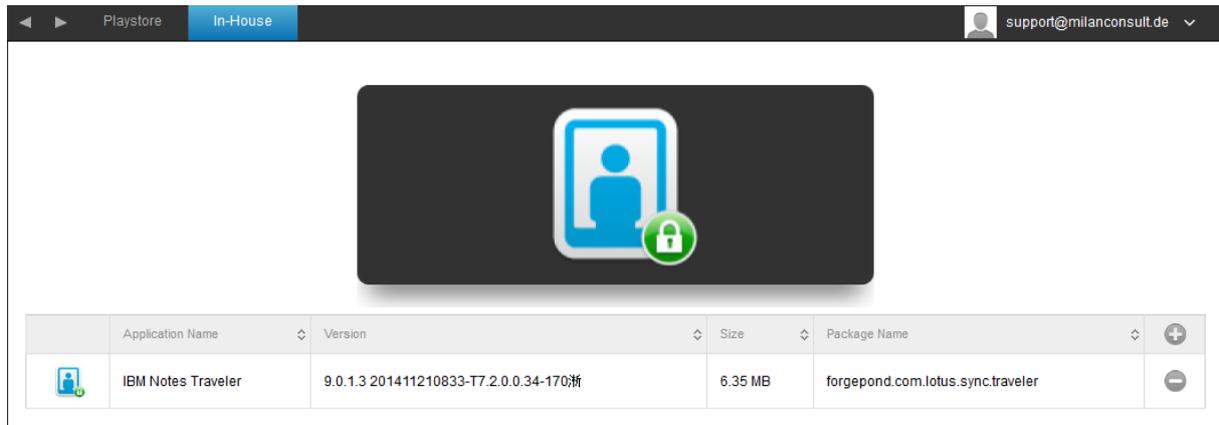
Wählen Sie nun mit „Durchsuchen...“ eine .apk Datei aus und klicken Sie anschließend auf „Upload“.



Ihre App wird nun hochgeladen, in der Mitte des Kreises können Sie eine Prozentanzahl sehen wie weit Ihre App bereits hochgeladen ist.



Sollte ein Upload der In-House App erfolgreich gewesen sein, können Sie nun die eben hochgeladen App in ihrem App Katalog vorfinden.



Der User ist nun in der Lage, auf seinem Endgerät diese App im AppTec Sore unter der Kategorie „In-House“ sehen und installieren zu können.

Da es sich hierbei um keine öffentliche Google PlayStore App handelt, braucht der User an seinem jeweiligen Endgerät keine hinterlegte Google ID.

Kiosk Mode

Der Kiosk Mode erlaubt es Ihnen eine App oder URL vorzudefinieren, dann ist es ausschließlich möglich diese App bzw. URL auszuführen/besuchen.

Ebenfalls können Sie im Kiosk Mode diverse Hardware tasten deaktivieren.

Automatic Start	Startet den Kiosk Mode automatisch, sobald das Profil auf dem Endgerät angekommen ist
Scheduled Kiosk Mode ?	Sie können anhand der Uhrzeit den Kiosk Mode planen, dieser wird dann in der von Ihnen definierten Uhrzeit automatisch gestartet und beendet
Start Time	Startzeit
Time in minutes	Zeit in Minuten, nachdem der Kiosk Mode wieder beendet werden soll
Application Type	Package
	URL
Package	Wenn Sie eine App im Kiosk Mode starten möchten, wählen Sie unter „Application Type“ „Package“ aus
Kiosk Application	Klicken Sie hier, um eine App die im Kiosk Mode gestartet werden soll auszuwählen Sie finden die gängige Übersicht vom App Management vor Sie können zwischen „Google Play Store“, „Android In-House Apps“ und einem „Packagename“ auswählen
URL	Wenn Sie eine URL im Kiosk Mode starten möchten, wählen Sie unter „Application Type“ „URL“ aus
URL	Definieren Sie hier nun Ihre gewünschte URL Adresse
Clear browser after inactivity	Hier können Sie einen Zeitintervall in Minuten definieren, nachdem nach einer Inaktivität der Kiosk Mode neu gestartet werden soll
Clear Web Cache and Cookies	Wenn Sie diese Funktion aktivieren, wird nach einem Neustart des Kiosk Modes der Web Cache (Cookies und cached Bilder) gelöscht
Same Origin Policy	Sollte diese Funktion aktiviert sein, kann der User nur unter Unterseiten der vordefinierten URL surfen z.B. haben Sie folgende URL definiert: www.mypage.com der User kann dann

	auf www.mypage.com/subpage surfen
Whitelisted URLs	Hier können Sie eine Whitelist pflegen, alle diese URLs sind zulässig Maximal 1 URL pro Linie Eine URL muss mit http:/ oder https:// beginnen
Blacklisted URLs	Hier können Sie eine Blacklist pflegen, alle diese URLs sind unzulässig Maximal 1 URL pro Linie Eine URL muss mit http:/ oder https:// beginnen
Screen Orientation	Diese Einstellung betrifft die Bildschirmdrehung Automatic = automatisch Portrait = Hochkant Format Landscape = Landschaftsmodus
Exit Password Enabled	Wenn Sie diese Funktion aktivieren, ist es dem User möglich, mit den von Ihnen vordefinierten Passwort den Kiosk Mode beenden zu können
Exit Password	Dies ist das von Ihnen vordefinierte Passwort
Disable Volume Keys	Deaktivieren der Lautstärke-Tasten (nur mit Samsung Geräte mit SAFE 3.0 oder höher verfügbar)
Disable On / Off Switch	Deaktivierung des An-/ Ausschalters (nur mit Samsung Geräte mit SAFE 3.0 oder höher verfügbar)
Disable Home Button	Deaktivierung des Home Buttons, wenn diese Funktion aktiviert wurde, kann der Kiosk Mode nur in der AppTec Console beendet werden (Nur mit Samsung Geräte mit SAFE 3.0 oder höher verfügbar)
Disable Navigation Bar	Hiermit können Sie die Navigation Bar deaktivieren (Zurück / Menü) Wenn diese Funktion aktiviert wird, kann der Kiosk Mode nur in der AppTec Console beendet werden (Nur mit Samsung Geräte mit SAFE 3.0 oder höher verfügbar)

Content Management

ContentBox

Unter diesem Punkt können Sie die ContentBox aktivieren.
Sobald Sie „Enable ContentBox“ auf „On“ geschaltet haben, wird eine separate ContentBox App automatisch auf dem Endgerät installiert.



Konfiguration Windows Phone

Je nachdem ob Sie aktuell ein Profil oder ein Gerät ausgewählt haben, unterscheidet sich die Darstellung und deren Unterpunkte – bitte beachten Sie dies sorgfältig!

General

Profile Information (nur auf Profil Ebene)

Sollten Sie sich in einem Profil befinden, erhalten Sie hier einen kurzen Überblick über das Profil in Bezug auf Name, OS, Erstellungsdatum, Autor, etc.

Profile Name	Name des Profils – kann direkt hier umbenannt werden
Operating System	Für welches Betriebssystem das Profil gilt
Created At	Erstelldatum
Created By	Ersteller des Profils
Last Change	Datum und Uhrzeit wann die letzten Änderungen am Profil vorgenommen wurden
Changed By	Anzeige darüber wer die letzte Änderung vorgenommen hat
Profile Revision	Anzahl wie oft das Profil bereits geändert wurde

Device Overview (nur auf Device Ebene)

Eine zusammenfassende Übersicht des ausgewählten Geräts, folgendes ist hier enthalten:

Device Name	Name des Geräts
Phone Number	Telefonnummer des Geräts
OS Version	OS Version des Geräts
Operating System	Betriebssystem (Android / iOS / Windows Phone)
Device Ownership	Firmen oder Privatgerät
Device Typ	Telefon oder Tablet
Rooted	Status ob das Gerät gerootet wurde
Compliant	Den Richtlinien entsprechend
Last Seen	Zeitpunkt an dem sich das Gerät zuletzt mit AppTec verbunden hat

Config Revision (nur auf Device Ebene)

Hier erhalten Sie eine Übersicht welches Gruppenprofil dem Gerät zugewiesen ist. Wenn sie auf das Gruppenprofil klicken, kommen Sie direkt zu diesem Profil und können Einstellungen vornehmen.

Mit dem  Symbol können Sie die zugewiesenen Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Mit dem  Symbol können Sie alle getätigten Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Device Log (nur auf Device Ebene)

Hier erhalten Sie diverse Gerätelogs.

Gegebenenfalls können Sie bei einem Fehler hier direkt die Ursache ausfindig machen.

Asset Management (nur auf Geräte Ebene)

Asset Management (nur auf Geräte Ebene)

Device Info

Manufacturer	Gerätehersteller
Model	Modellbezeichnung des Geräts
Operating System	Betriebssystem
OS Version	Betriebssystem Version
Free / Total Memory	Freier / Gesamter Speicherplatz
Display Resolution	Bildschirmauflösung
Phone Language	Sprache des Gerätes
Firmware Version	Firmware Version
DM Client Revision	Device Management Client Version
Hardware Version	Version der Hardware im Gerät
CPU Architecture	CPU Architektur (Typ des Prozessors)

Wi-Fi

WiFi MAC	WiFi MAC Adresse
----------	------------------

Cellular

SIM Carrier Network	Netzanbieter
IMSI	<p>Die International Mobile Subscriber Identity (IMSI; deutsch Internationale Mobilfunk-Teilnehmerkennung) dient in GSM- und UMTS-Mobilfunknetzen der eindeutigen Identifizierung von Netzteilnehmern</p> <p>Die IMSI besteht aus maximal 15 Ziffern und setzt sich folgendermaßen zusammen: [1]</p> <ul style="list-style-type: none"> • Mobile Country Code (MCC), 3 Ziffern • Mobile Network Code (MNC), 2 oder 3 Ziffern <p>Mobile Subscriber Identification Number (MSIN), 1-10 Ziffern</p>
Modem Firmware	Modem Firmware

Synchronization Info

Instant DM Connection	Das Gerät soll sofort nach dem Einrollen eine Verbindung zu AppTec aufbauen
Initial Retry Time	Retry Zeit für diese erste Verbindung
Connection Retries	Anzahl der erneuten

	Verbindungsversuche nach einem Abbruch durch den Connection Manager oder einem WinInet-level Fehler
Maximum Sleep Time	Maximale Wartezeit nach package-sending Fehler
First Sync Retries	Zeit für die erste Stage nach dem Enrollment
First Retry Interval	Zeit für die erste Stage nach dem Enrollment
Second Retry Interval	Zeit für zweite Stage nach dem Enrollment
Regular Sync Retries	Zeit für weiteren Stage nach dem Enrollment
Regular Retry Interval	Zeit für weiteren Stage nach dem Enrollment

Security Management

Security Configuration

Passcode

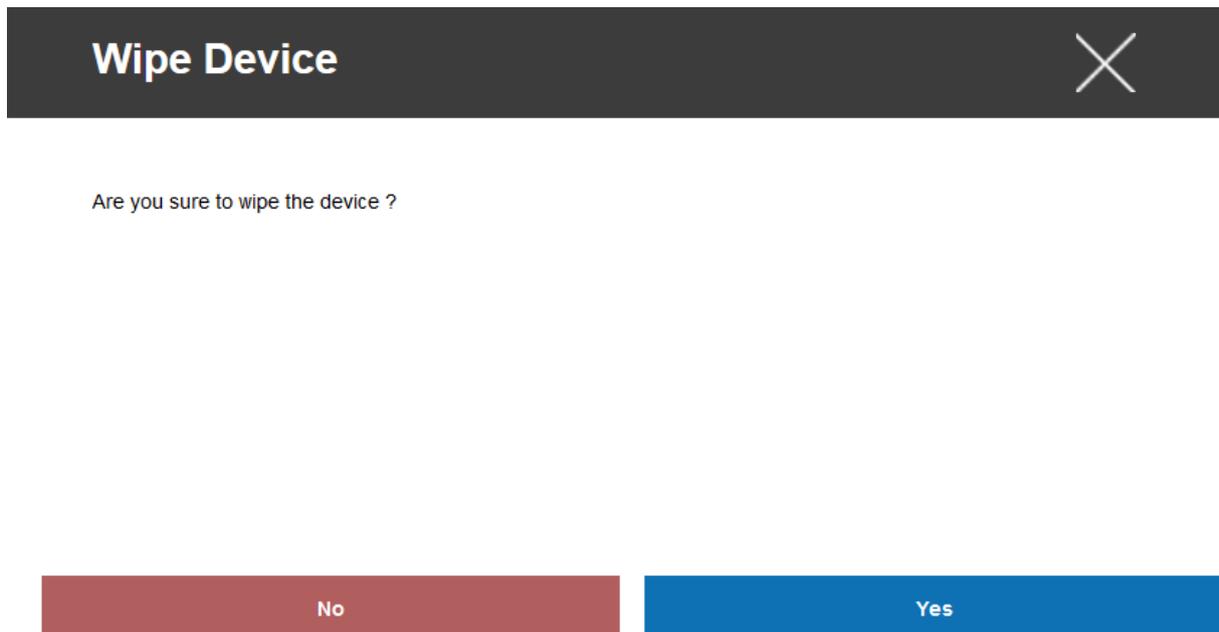
Allow Simple Passwords	Erlauben von simplen Passwörtern, wie z.B. 1234 oder 1111
Minimum Password Length	Mindestanzahl an Zeichen des Passworts
Password Composition	Spezifizieren die Anzahl wie viel Charaktereigenschaften das Passwort besitzen muss Diese setzen sich aus Großbuchstaben, Kleinbuchstaben, Nummern und Sonderzeichen zusammen
Password Quality	Hier können Sie die Passwort Qualität einstellen Alphanumeric = Nur Zahlen und Buchstaben Numeric = Nur Zahlen Numeric or Alphanumeric = Zahlen oder Zahlen und Buchstaben
Maximum Inactivity Time Lock	Anzahl in Minuten, nachdem das Gerät ohne das Zutun des Users (Inaktivität) gesperrt werden soll Der User muss nach dieser Zeit das Gerät entsperren, indem er seine Gerätepasswort eingibt
Password Expiration	
Password History Restriction	Anzahl der wie viel zuletzt benutzten Passwörter nicht erlaubt ist
Maximum Failed Password Attempts	Anzahl wie oft das Passwort falsch eingegeben werden darf, bis ein vollständiger Wipe des Gerätes durchgeführt wird
Allow Password Grace Period Timer	Wennj aktiv, kann der User die Zeit zu erneuten Passworteingabe einstellen. Wenn nicht, so wird das Passwort immer angefordert.

End of Life (nur auf Geräte Ebene)

Wipe (nur auf Geräte Ebene)

Unter „Wipe“ können Sie das Gerät auf die Werkseinstellungen zurücksetzen, hier werden sowohl die geschäftlichen, als auch die privaten Daten auf dem Endgerät gelöscht

Mit dem Klick auf das „Minussymbol“  sollten Sie folgende Meldung erhalten



Mit „Yes“ können Sie die *Löschung durchführen*.

Unter „Wipe Report“ können Sie sich folgende Dinge anzeigen lassen

Wiped by	Historie von wem der Wipe ausgeführt wurde
Date	Datum
Status	Status (z.B. ob der Wipe erfolgreich durchgeführt wurde)

Restriction Settings

Device Functionality

Allow SD Card	Erlauben einer SD Karte
Allow Camera	Erlauben der Kamera
Enable Storage Encryption	Verschlüsselt die internen Daten auf dem Endgerät, falls diese Funktion einmal aktiviert wurde ist es nicht mehr möglich dies rückgängig zu machen SD Karten werden nicht verschlüsselt!
Allow USB Connection	Erlauben von USB Verbindungen
Allow Voice Recording	Erlauben von Sprachaufnahmen
Allow Location Service	Erlaubt die Lokalisierung des Endgerätes
Allow Screen Capture	Erlauben von Screenshots
Allow Developer Unlock	Erlaubt den Entwicklungsmodus
Allow AntiTheft Mode	Erlaubt es dem User „Mein Handy finden“ zu nutzen, sollte diese Funktion bereits vor der Deaktivierung genutzt worden sein, muss sie zuerst manuell am Endgerät deaktiviert werden
Allow Cellular Data Roaming	Erlauben von mobilen Daten im im Roaming
Allow Cortana	Erlaubt den Sprachassistenten Cortana
Allow Appstore	Erlauben des offiziellen Appstores
Celluar App Download Limit	Maximal erlaubte App-Größe zum Download über das Mobilfunknetz
Allow Browser	Erlaubt den nativen Browser
Allow Task Switcher	Erlauben des Task-Managers
Allow Search to use Location	Erlaube der Suche, Lokalisierungsdaten zu verwenden
Allow Moderate Search Filter	Solle diese Funktion aktiviert werden, werden nicht jugendfrei Inhalte herausgefiltert und verhindert
Allow Storing Images From Vision Search	Mit dieser Einstellung können Sie verhindern, dass am Endgerät QR Code als Bilder gespeichert werden dürfen Ausschließlich der aktuell gescannte Code befindet sich auf dem Endgerät
Allow Save As Office Files	Erlaubt es dem User eine Datei als Office-Datei zu speichern Diese Policy betrifft nur den Office Hub
Allow Sharing Of Office Files	Erlaubt es dem User Office Dateien zu teilen Diese Policy betrifft nur den Office Hub
Allow Action Center Notificions	Erlaubt das Anzeigen von Nachrichten im Action Center bei Sperrung
Allow Sync My Settings	Erlaubt die Synchronisierung von Einstellungen geräteübergreifend

<p>Enable Email Data Encryption</p>	<p>Aktiviert die Datenverschlüsselung von E-Mails und deren Anhänge Das Gerätepasswort wird benötigt, um diese Dateien entschlüsseln zu können</p>
<p>Allow User Reset</p>	<p>Erlaubt es dem User sein Gerät in den Einstellungen oder mit den Hardware Tasten zurückzusetzen ACHTUNG! Diese Einstellung sollte nur dann deaktiviert werden, wenn es sich hierbei um ein Firmengerät handelt Sollte das Gerät aus welchen Gründen auch immer keine Verbindung mit dem AppTec Server mehr aufbauen können, muss das Gerät in einen Nokia Store geschickt werden, um das Gerät auf die Werkeinstellungen zurückzusetzen können Microsoft kann hierfür nicht für ein solches Problem verantwortlich gemacht werden</p>
<p>Allow User Unenrollment</p>	<p>Erlaubt es dem User den Unternehmensbereich zu entfernen und somit die Verbindung zu den AppTec Servern zu trennen, sollte dies geschehen ist es nicht mehr möglich das Geräte zu managen ACHTUNG! Diese Einstellung sollte nur dann deaktiviert werden, wenn es sich hierbei um ein Firmengerät handelt Sollte das Gerät aus welchen Gründen auch immer keine Verbindung mit dem AppTec Server mehr aufbauen können, muss das Gerät in einen Nokia Store geschickt werden, um das Gerät auf die Werkeinstellungen zurückzusetzen können Microsoft kann hierfür nicht für ein solches Problem verantwortlich gemacht werden</p>

Connection Management

Wifi

Nehmen Sie an dieser Einstellung die Vorkonfiguration der Endgeräte für den Zugriff auf interne Access Points vor

Service Set Identifier (SSID)	SSID des zu verbindenden Netzwerks
Auto Join	Automatischen Beitreten zum Netzwerk aktivieren
Hidden Network	Aktivieren, falls der AP die SSID nicht broadcastet
Security Type	Sicherheitstyp des AP festlegen
WEP Open System	
Password	Passwort für den AP
WPA PSK	
Password	Passwort für den AP
WPA EAP	
Authentication Type	Authentifizierungsmöglichkeit, nur „PEAP-MSCAHPv2“ möglich
Fast Reconnect	Geräte können zwischen den Access Points wechseln, ohne sich erneut authentifizieren zu müssen
Guest Access	Der User hat keinen Account und soll sich somit als Gast anmelden
Quarantine Checks	Der Client muss NAP (Network Access Protection) Checks ausführen und das Ergebnis dem System mitteilen, welches dann entscheidet ob sich der Client verbinden darf
Require Crypto Binding	Ausschließlich eine Authentifizierung über die Cryptobinding möglich
Server Validation	Der Client überprüft, ob das Server Zertifikat gültig ist, falls dies der Fall ist wird eine Verbindung hergestellt
Prompt for Certificates	Erlaubt dem Benutzer nicht vertrauenswürdige Zertifikate zu akzeptieren
Anonymous User Name	Der Client sendet seine Identität erst dann, sobald der RADIUS Server authentifiziert wurde Bis dahin nutzt er die hier angegebene Identität
Logon Domain	Domaine zum Einloggen
User Name	Benutzername
Password	Passwort
Server Names	Bietet die Möglichkeit den Name des RADIUS-Servers anzugeben, der die Netzwerkauthentifizierung und –

	autorisierung bereitstellt
WPA2-PSK	
Password	Passwort für den AP
WPA2 EAP	
Authentication Type	Authentifizierungsmöglichkeit, nur „PEAP-MSCAHPv2“ möglich
Fast Reconnect	
Guest Access	
Quarantine Checks	Aktiviert den Netzwerk Zugriffsschutz NAP
Require Crypto Binding	Ausschließlich eine Authentifizierung mit Server die cryptobinding möglich
Server Validation	
Prompt for Certificates	Verlangt nach einem validierten Server-Zertifikat, Name oder einer Root Zertifikatsauthentifizierung (CA)
Anonymous User Name	
Logon Domain	
User Name	Benutzername
Password	Passwort
Server Names	Auflistung deren Server, deren Geräte vertraut werden soll
None	Keine Sicherheit festgelegt
Use Proxy Server	Das Benutzen eines Proxy Servers
Server Address	Serveradresse des Proxy Servers
Server Port	Server Port des Proxy Servers

Wifi Restrictions

Hier können Sie diverse Wifi Restriktionen definieren.

Allow WiFi	Erlauben bzw. verbieten von WiFi
Allow Internet Sharing	Erlauben eines Hotspots
Allow Auto Connect to WiFi Sense Hot Spots	Erlauben von automatischen Verbindungen zu einem WiFi Sense Hot Spots
Allow WiFi Hot Spot Reporting	Erlauben das WiFi Hotspot Informationen an Microsoft versendet werden dürfen
Allow Manual WiFi Configuration	Erlaubt es dem User sich mit nicht von AppTec definierten WiFi Netzwerken zu verbinden
WLAN Scan Frequency	Legt den WLAN-Scan Intervall fest, dabei verbessert ein höherer Wert die Erkennung von Wifi-Netzwerken

VPN

Nehmen Sie hier die entsprechenden Einstellungen vor, um die VPN Verbindungen zu konfigurieren

Connection Name	Angezeigte VPN Verbindungsname
Server	Serveradresse des VPN Servers
VPN Type	Typ der Verbindung
IKEv2 (native)	Es wird eine native VPN Verbindung genutzt
SSL-VPN (third-party)	Es wird eine 3rd Party App genutzt
Third-Party App	
	JunOS Pulse
	SonicWall Mobile Connect
	F5 Big-IP Edge Client
	Checkpoint Mobile VPN
Third-Party Configuration File	Hier muss der Inhalt der Konfigurationsdatei eingefügt werden
Authentication Type	Authentifizierungsmethode
Bypass Local Traffic	Bei Zugriff auf interne Ressourcen wird der Verkehr nicht über die VPN Verbindung geleitet
Connection Type	Manual = Der User muss manuell eine VPN Verbindung aufbauen / beenden Triggering = Die VPN Verbindung wird automatisch aufgebaut, sobald eine App sich zu einer geschützten oder internen Ressource verbinden möchte Dies ist die empfohlene Einstellung seitens AppTec um die bestmögliche Benutzung zu gewährleisten
Trusted Network Detection	Wenn diese Funktion aktiviert ist, wird keine VPN Verbindung aufgebaut, solange der User sich im Firmen-WiFi befindet, da geschützte Ressourcen direkt auf dem Endgerät erreichbar wären Sollte diese Funktion deaktiviert sein, wird eine VPN Verbindung über das Firmennetzwerk aufgebaut Es muss eine DNS Suffix eingerichtet werden, um zu definieren bei welchem WiFi es sich um eine Firmen-WiFi handelt
DNS Suffix	Hier können Sie den primären DNS Suffix eintragen
Use Proxy	Die Benutzung eines Proxys
Server Address	Serveradresse des Proxy Servers
Server Port	Server Port des Proxy Servers
Bypass Local Traffic	Bei Webanfragen ins lokale Intranet wird

	der Verkehr nicht über den Proxy geleitet.
--	--

VPN Restrictions

Hier können Sie diverse VPN Restriktionen definieren.

Allow Manual VPN Configuration	Diese Richtlinie erlaubt bzw. verbietet dem User die VPN Einstellungen zu deaktivieren und zu verändern
Allow VPN over Cellular	Verbietet bzw. erlaubt dem Gerät eine VPN Verbindung aufzubauen, falls sich das Gerät mobile Daten nutzt
Allow VPN Roaming over Cellular	Verbietet bzw. erlaubt dem Gerät eine VPN Verbindung aufzubauen, falls sich das Gerät im Roaming befindet

Bluetooth

Hier können Sie festlegen, ob Bluetooth erlaubt bzw. nicht erlaubt werden soll.

Allow Bluetooth	Bluetooth aktivieren / deaktivieren
-----------------	-------------------------------------

NFC

Unter diesem Punkt können Sie festlegen, ob NFC erlaubt bzw. nicht erlaubt sein soll.

Allow NFC	NFC aktivieren / deaktivieren
-----------	-------------------------------

PIM Management

Exchange Active Sync

Einrichten eines ActiveSync Kontos am Endgerät

Account Name	Name des Email Accounts
Server Host Name	Adresse/FQDN des Servers
Domain Name	Domäne des Servers
Email Address	E-Mail Adresse
User Name	Benutzername
User Password	Sie können hier optional bereits dem User ein Passwort mitgeben
Use SSL	Nutzung einer SSL Verbindung
Sync Interval	Hier kann das Intervall für die Synchronisation festgelegt werden Manual sync = Der User muss seine Mails aufrufen und eine manuell Synchronisation durchführen
Mail Age Filter	Zeitraum bis wann die Mails synchronisiert werden sollen No filter = unbegrenzt
Log Level	Festlegung der Logginglevels für den ActiveSync Verkehr
Sync Email	Aktiviert = Mails werden synchronisiert
Sync Contacts	Aktiviert = Kontakte werden synchronisiert
Sync Calendar	Aktiviert = Kalender wird synchronisiert
Sync Tasks	Aktiviert = Aufgaben werden synchronisiert

eMail

Einrichten von POP3/IMAP4 Konten am Endgerät.

Account Description	Name des Email Accounts
Sender Name	Angezeigter Name des Senders
Domain Name	Domainname für den Email Account
Email Address	Email Adresse des Benutzers
User Name	Benutzername
User Password	Sie können hier optional bereits dem User ein Passwort mitgeben
Alternative Outgoing Server Credentials	Hier kann definiert werden, falls für den ausgehenden Server andere Credentials benötigt werden
Outgoing Domain Name	Ausgehende Domainname
Outgoing Server User Name	Ausgehender Benutzername
Outgoing Server Password	Ausgehendes Passwort
Email Protocol	POP3 oder IMAP4 kann als Protokoll genutzt werden
Incoming Mail Server Host Name	Eingehender Server Hostname
Use SSL for Incoming Mails	Benutzung von SSL bei eingehenden Mails
Outgoing Mail Server Host Name	Ausgehender Server Hostname
Use SSL for Outgoing Mails	Benutzung von SSL bei ausgehenden Mails
Outgoing Server Authentication	Eine ausgehende Server Authentifikation wird benötigt
Sync Interval	Hier kann das Intervall für die Synchronisation festgelegt werden Manual sync = Der User muss seine Mails aufrufen und eine manuell Synchronisation durchführen
Mail Age Filter	Zeitraum bis wann die Mails synchronisiert werden sollen No filter = unbegrenzt

App Management

Enterprise App Manager

Installed Apps (nur auf Geräte Ebene)

Hier werden Ihnen alle In-House Apps angezeigt.

Sie können direkt über das  Symbol eine neue In-House App (.xap Datei) dem Endgerät zuweisen.

Mandatory Apps

Hier werden Ihnen alle „Mandatory Apps“, also sprich zwingend auf dem Endgerät erforderliche Apps angezeigt.

Sie können über das  eine weitere Mandatory In-House App festlegen.

Whitelisted / Blacklisted Apps

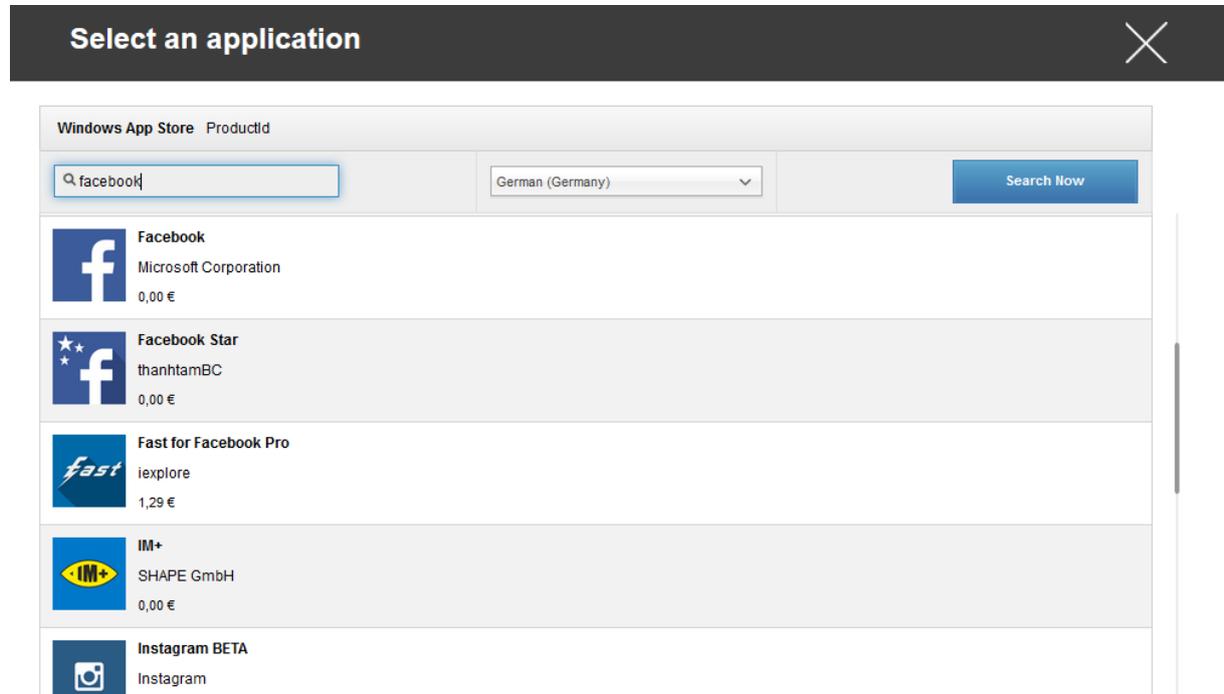
Je nachdem ob Sie unter „General Settings“ > „Black- & Whitelisting“ > „Windows“ > „Blacklisting“ oder „Whitelisting“ ausgewählt haben, können Sie hier blacklisted oder whitelisted Apps definieren.

Blacklisted Apps bedeutet dass all diese Apps nicht auf dem Endgerät installiert bzw. ausgeführt werden können, alle Apps die nicht hier definiert werden können installiert und ausgeführt werden

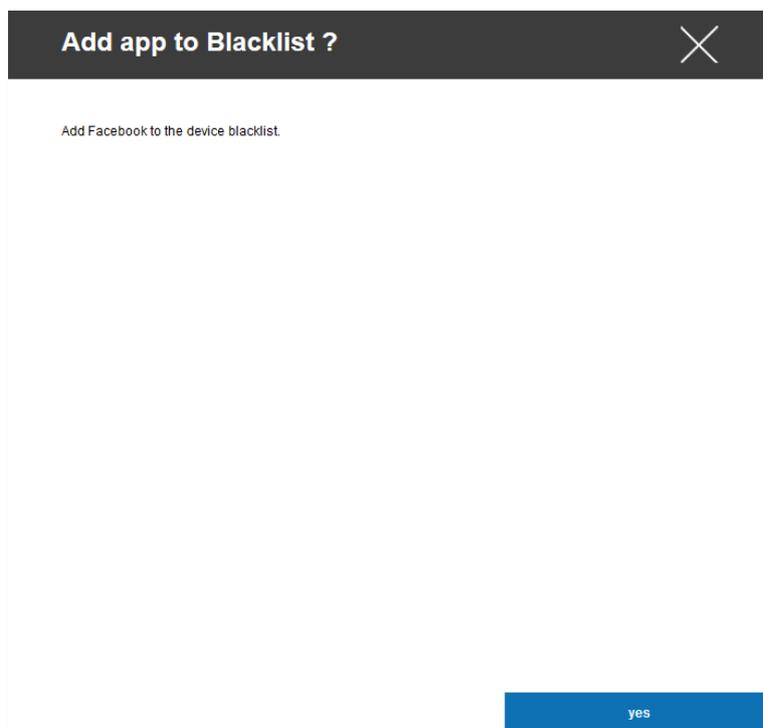
Whitelisted Apps bedeutet dass nur diese vordefinierten Apps installiert bzw. ausgeführt werden können.

Ebenfalls über das  können weitere Windows Apps oder Product IDs festgelegt werden. Suchen Sie einfach nach einer App, in unserem Beispiel wäre dies Facebook.

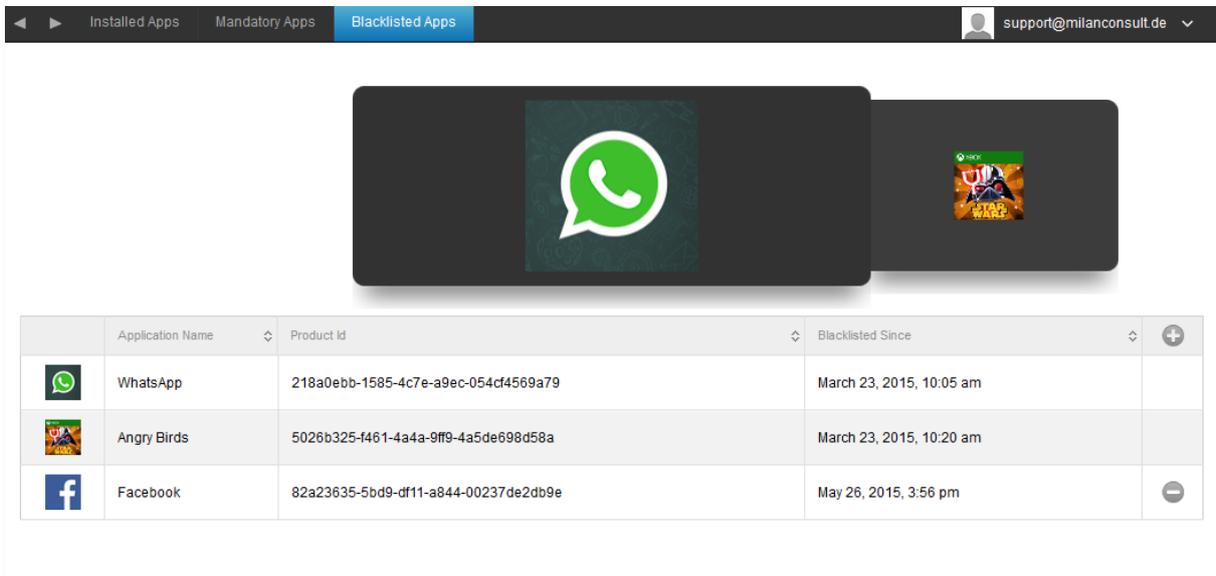
Klicken Sie anschließend auf das App-Icon oder auf den Name der jeweiligen App.



Anschließend öffnet sich folgendes Fenster, bestätigen Sie dies mit „yes“.



Sollte der App-Import erfolgreich gewesen sein, können Sie nun die eben definierte App in der Übersicht vorfinden.



	Application Name	Product Id	Blacklisted Since	
	WhatsApp	218a0ebb-1585-4c7e-a9ec-054cf4569a79	March 23, 2015, 10:05 am	
	Angry Birds	5026b325-f461-4a4a-9ff9-4a5de698d58a	March 23, 2015, 10:20 am	
	Facebook	82a23635-5bd9-df11-a844-00237de2db9e	May 26, 2015, 3:56 pm	

In unserem Beispiel, da wir hier mit „Blacklisted Apps“ arbeiten wäre es uns jetzt nicht möglich „Whatsapp“, „Angry Birds“ und „Facebook“ zu installieren bzw. auszuführen, falls eine dieser Apps bereits vor dieser Regelung auf dem Endgerät installiert waren.

Enterprise App Store

Windowsstore

Hier sind Sie in der Lage Windows Apps an die User zu verteilen. Es handelt sich hierbei um öffentliche Windows Apps und können von dem jeweiligen User optional über den AppTec Enterprise AppStore installiert werden.

Über das  Symbol lassen sich weitere Windows Apps hinzufügen.
 Über „Enter Searchterm here ...“ können Sie nach einer App aus dem Windows Store suchen. In unserem Beispiel handelt es sich hierbei um die „DB Navigator“ App.

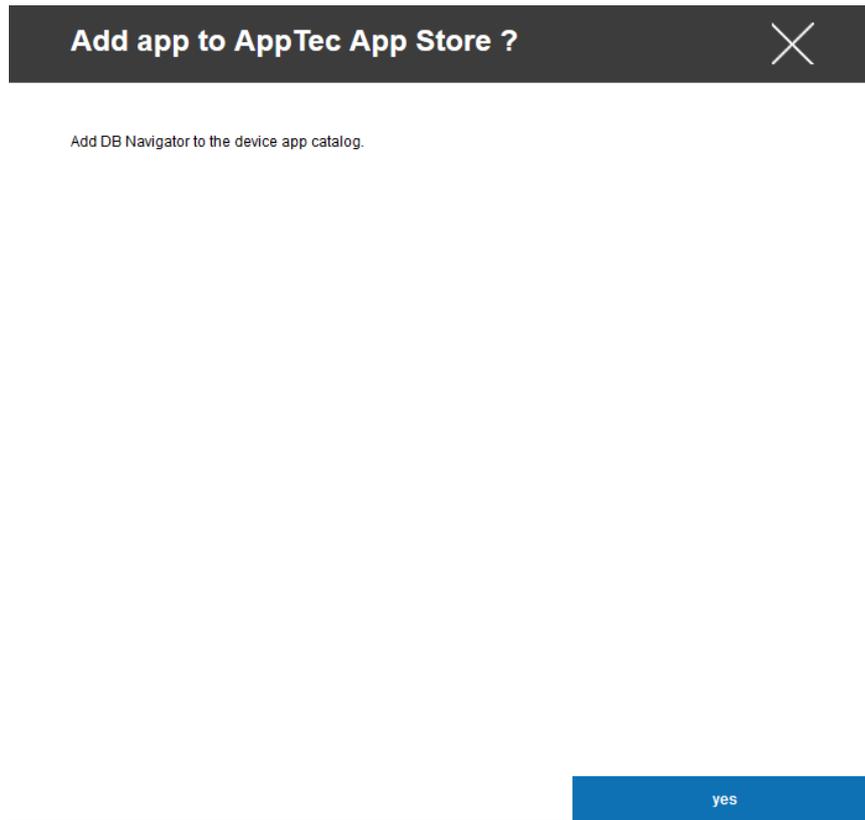
Select an application
✕

Windows App Store

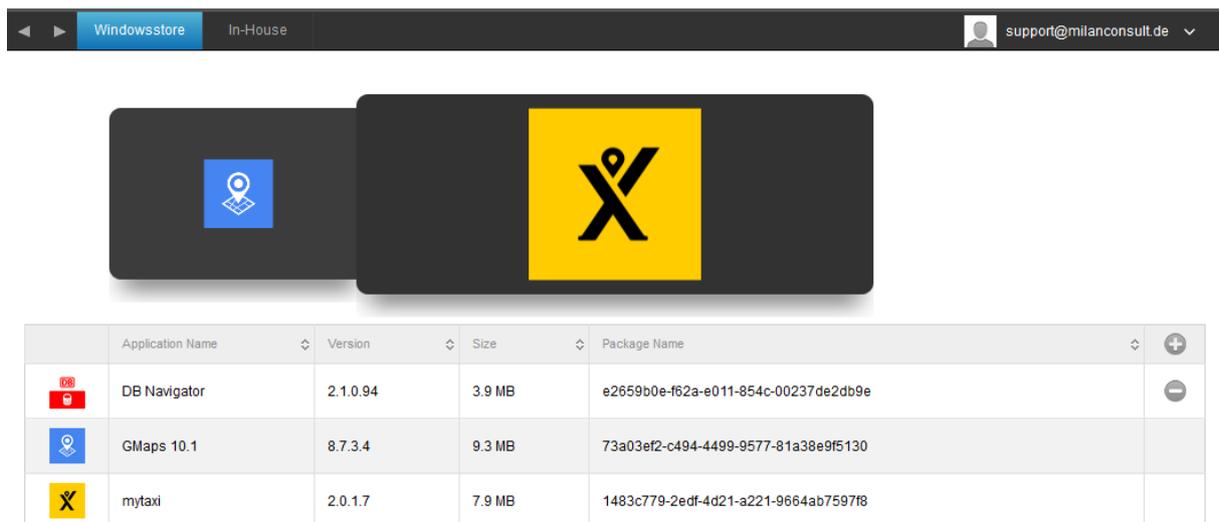
▼

	DB Navigator Deutsche Bahn 0,00 €
	FahrPlaner Verkehrsverbund Bremen Niedersachsen 0,00 €
	Flinkster - Carsharing DB Rent GmbH 0,00 €
	JDB for Facebook JDB Pocketware 0,00 €
	Navi S-Bahn München Deutsche Bahn

Anschließend öffnet sich folgendes Fenster, bestätigen Sie dies mit „yes“.



Sollte der App-Import erfolgreich gewesen sein, können Sie nun die eben definierte App in der Übersicht vorfinden.

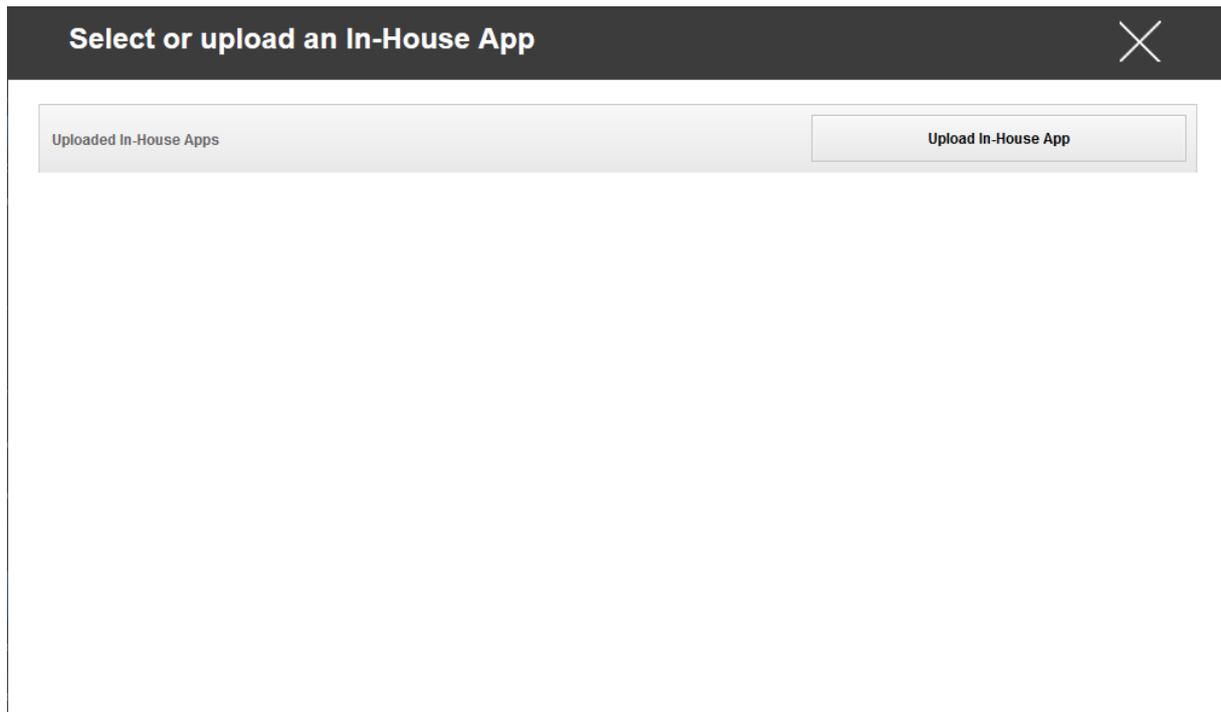


In-House

Hier sind Sie in der Lage In-House Apps an die User zu verteilen. Es handelt sich hierbei um eigenentwickelte Windows Apps und können von dem jeweiligen User optional über den AppTec Enterprise AppStore installiert werden.

Über das  Symbol lassen sich weitere In-House Windows Apps hinzufügen.

Klicken Sie im sich drauf öffnenden Fenster „Upload In-House App“.



Klicken Sie nun auf „Durchsuchen...“ und wählen Sie eine .xap Datei aus.

Upload an In-House App [X]

Upload Limit: max. size of xap files is 50 MB
Select the .xap file of the windows phone application which you want to upload

Keine Datei ausgewählt.

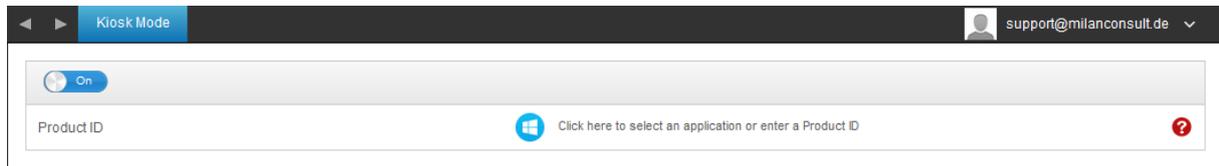
Nachdem Sie die xap Datei ausgewählt haben, können Sie mit „Upload“ die App in Ihren AppTec Enterprise AppStore importieren.

Sollte der Upload erfolgreich gewesen sein, können Sie die App nun in der Übersicht vorfinden.

Kiosk Mode

Kiosk Mode

Unter dem Punkt „Kiosk Mode“ können Sie eine App in den Vollbildmodus bringen, anschließend ist es nur noch möglich diese App zu nutzen.

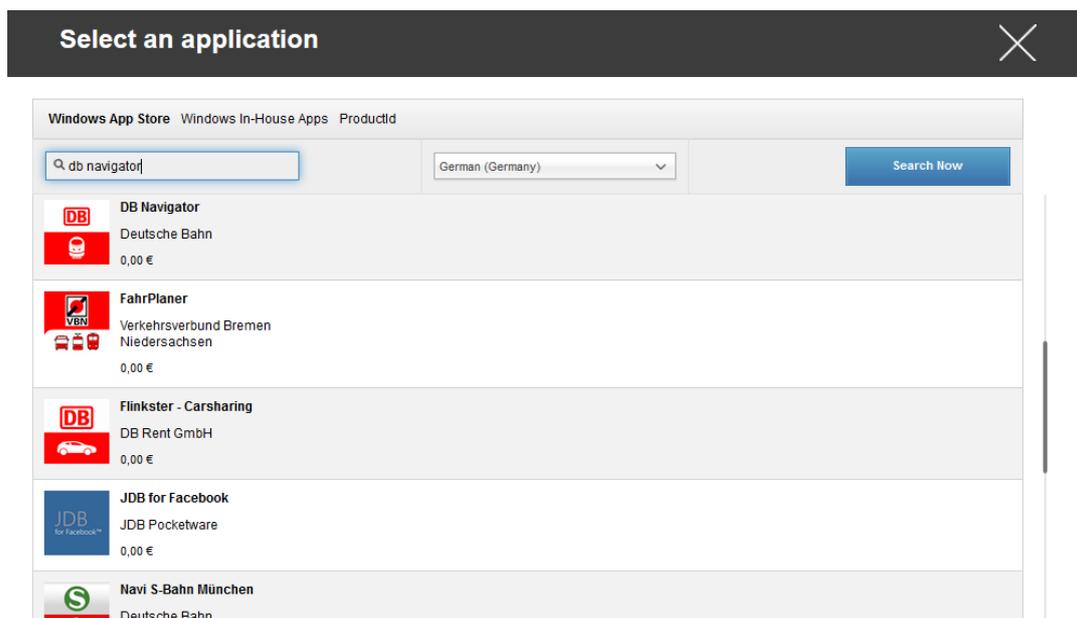


ACHTUNG!

Der Kiosk Mode unter Windows Phone kann nur dann deaktiviert werden, indem das Gerät auf die Werkseinstellungen zurückgesetzt wird.

Die App / Product ID die hier definiert wird, wird nach jedem Geräte Neustart automatisch im Vollbild ausgeführt.

Mit „Click here to select an application or entere a Product ID“ können Sie eine öffentliche / In-House Windows App definieren oder Sie sind ebenfalls in der Lage



eine Product ID festzulegen.

Denken Sie daran die Kiosk Mode App ebenfalls unter „Mandatory App“ festzulegen.

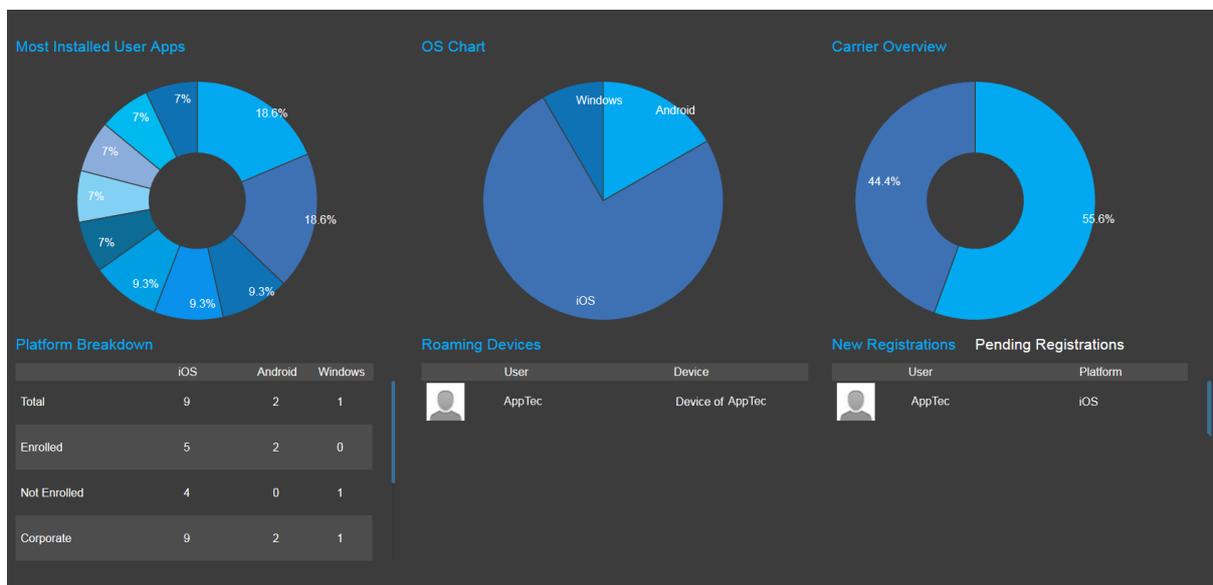


V. Dashboard & Reporting

Dashboard

Das „Dashboard“ zeigt Ihnen grundlegende Informationen auf einen Blick an:

- Meist installierten Apps
- Aktueller Status der Endgeräte
- Übersicht der aktuellen Plattformen
- Geräte die Roaming aktiviert haben
- Genutzter Netzanbieter
- Neue Registrierungen / ausstehende Registrierungen



Extended Reporting

Das „Extended Reporting“ bringt detaillierte und informationsreiche Ansichten, Grafiken und Übersichten mit.

In der Regel finden Sie in den Unterpunkten folgende Tabs:

- All (Alle Geräte)
- iOS (nur iOS Geräte)
- Android (nur Android Geräte)
- ggfs. Windows (nur Windows Phone Geräte)
- Bei Ausnahmefällen wird dies explizit in dem jeweiligen Unterpunkt erwähnt

Unter dem jeweiligen Unterpunkt können Sie sich mit  (Export Data) die aktuelle Übersicht als .csv Datei exportieren lassen.

Sollte der Unterpunkt eine Grafik enthalten, können Sie mit  (Hide Chart) die Grafik ausblenden, bzw. mit  (Show Chart) die Grafik (wieder) einblenden.

Folgende Punkte sind standardmäßig vorzufinden:

Device Alias	Gerätename
Device Owner	Besitzer des Gerätes
eMail	E-Mail Adresse des Gerätes
Phone	Telefonnummer
OS	Betriebssystem
Last Seen	Zuletzt beim AppTec Server gemeldet

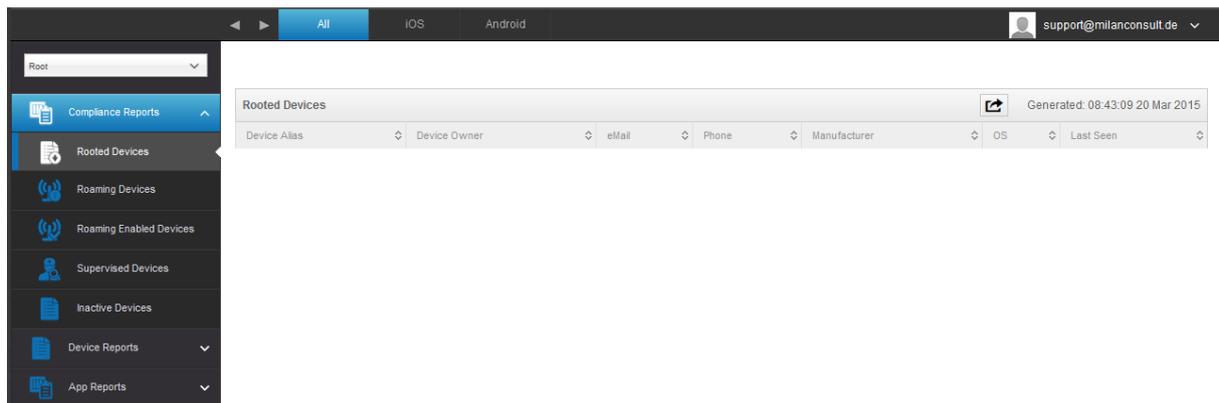
Compliance Reports

Rooted Devices

Übersicht aller Geräte die gerootet / ge jailbreakt wurden.

Zusätzlicher Punkt in dieser Kategorie:

Manufacturer	Gerätehersteller
--------------	------------------



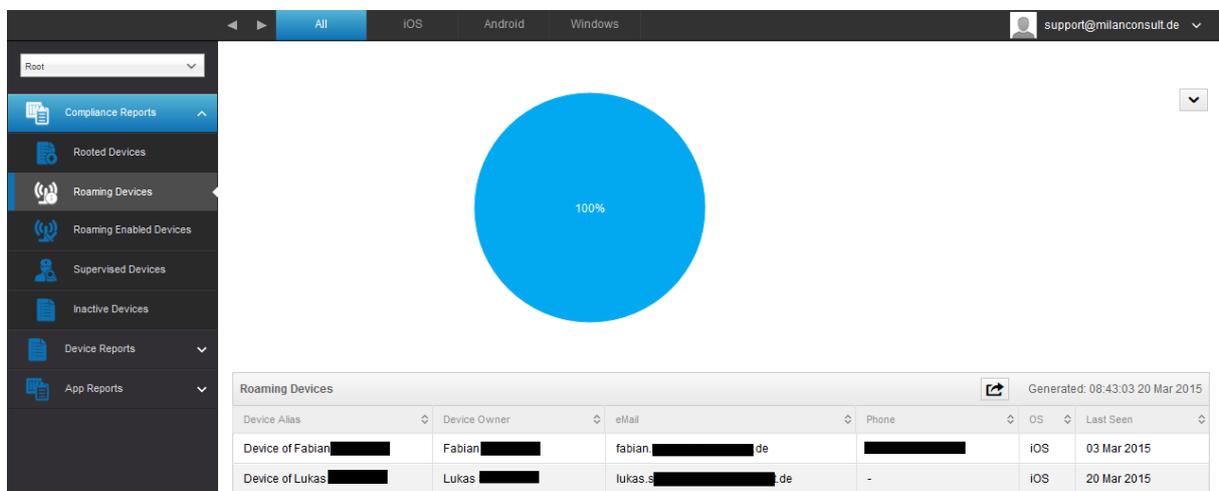
Device Alias	Device Owner	eMail	Phone	Manufacturer	OS	Last Seen

Roaming Devices

Übersicht aller Geräte die sich im Roaming befinden.

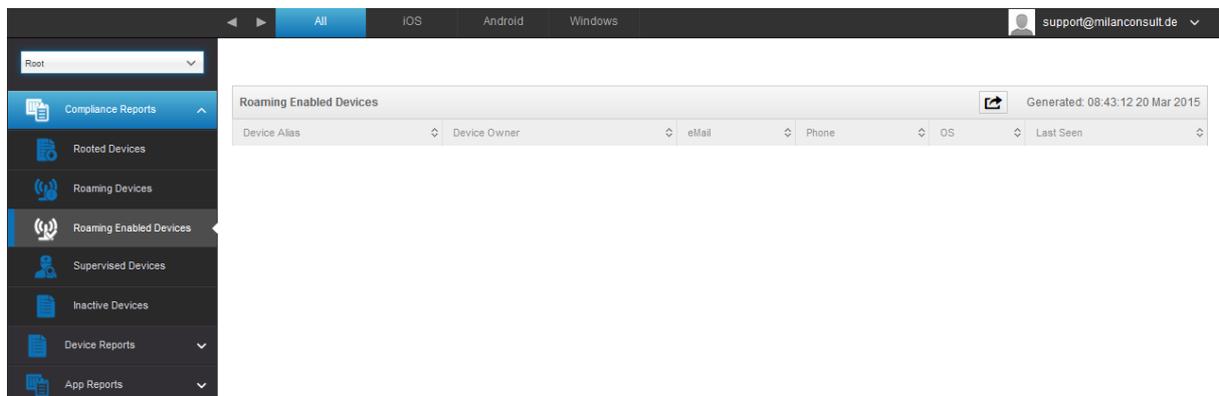
Zusätzlicher Punkt in dieser Kategorie:

Phone	Telefonnummer
-------	---------------



Device Alias	Device Owner	eMail	Phone	OS	Last Seen
Device of Fabian [REDACTED]	Fabian [REDACTED]	fabian.[REDACTED]@de	[REDACTED]	iOS	03 Mar 2015
Device of Lukas [REDACTED]	Lukas [REDACTED]	lukas.s[REDACTED]@de	-	iOS	20 Mar 2015

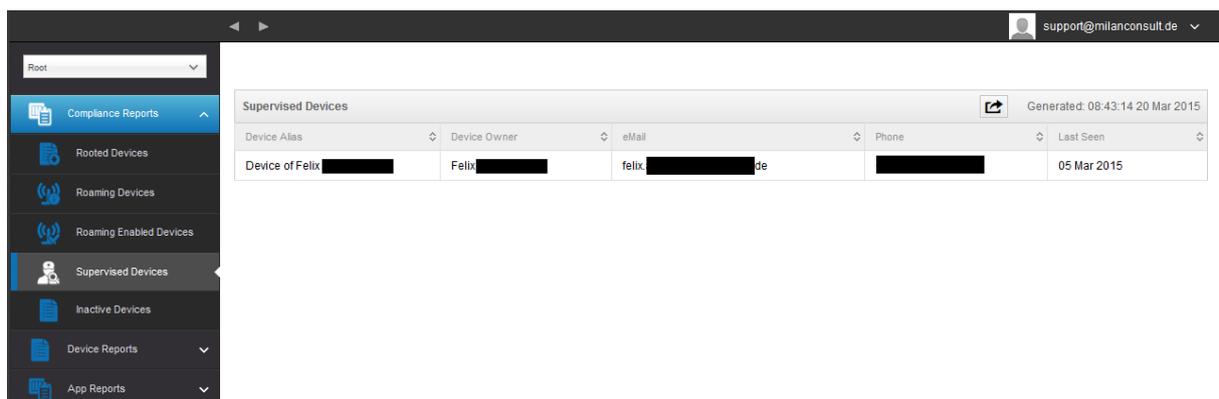
Roaming Enabled Devices



Übersicht aller Geräte die Romaing aktiviert haben.

Supervised Devices

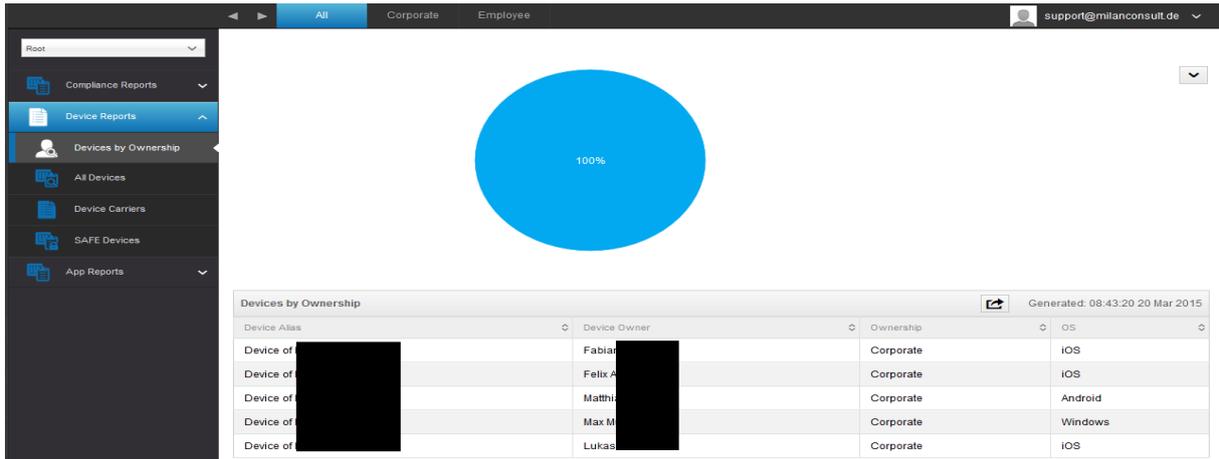
Alle Geräte die Supervised sind (ausschließlich iOS Geräte)



Hier können Sie sehen wie viel Geräte aktuell Corporate (Firmengeräte) und Employee (Privatgeräte) im Einsatz sind.

Zusätzlicher Punkt:

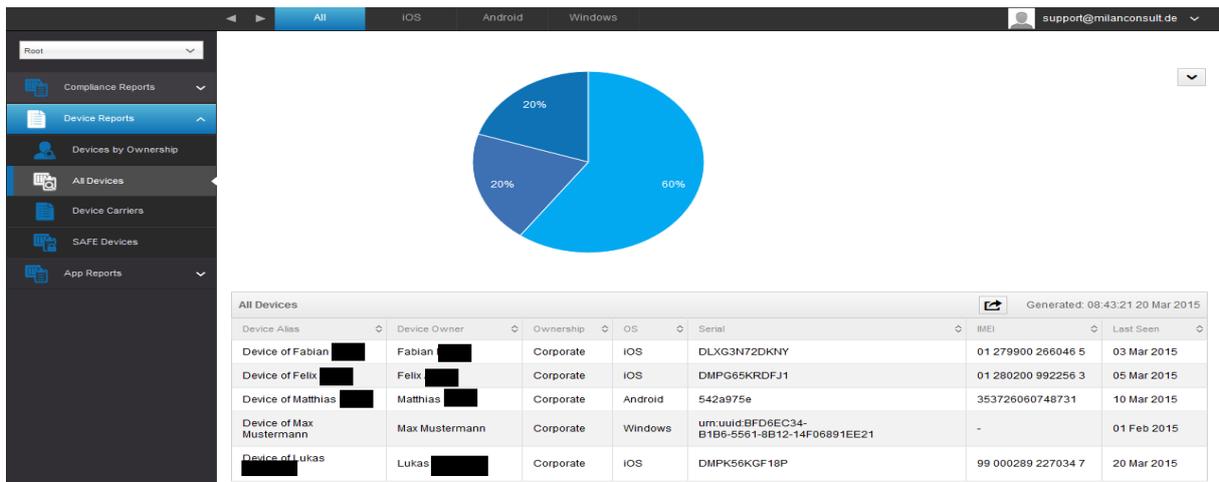
Ownership	Corporate = Firmengerät Employee = Privatgerät
-----------	---



All Devices

Hier finden Sie eine Übersicht von allen Geräten mit den wichtigsten Informationen.

Zusätzliche Punkte:



Ownership	Corporate = Firmengerät Employee = Privatgerät
Serial	Serialnummer des Gerätes
IMEI	IMEI Nummer des Gerätes

Device Carriers

Hier erhalten Sie eine Übersicht in Hinsicht auf den Carrier (Mobilfunkanbieter).

Zusätzliche Punkte:

Carrier	Mobilfunkanbieter z.B. Telekom, Vodafone
---------	---

SAFE Devices

Hier erhalten Sie eine Übersicht welche Geräte welche SAFE Version nutzen. Da diese Übersicht bzw. SAFE nur für Samsung Geräte verfügbar ist, sehen Sie in diesem Punkt nicht die üblichen Tabs.

Zusätzliche Punkte in dieser Kategorie:

Phone	Telefonnummer
SAFE Version	SAFE Version

App Reports

Hier erhalten Sie alle möglichen Übersichten in der Hinsicht auf Apps.

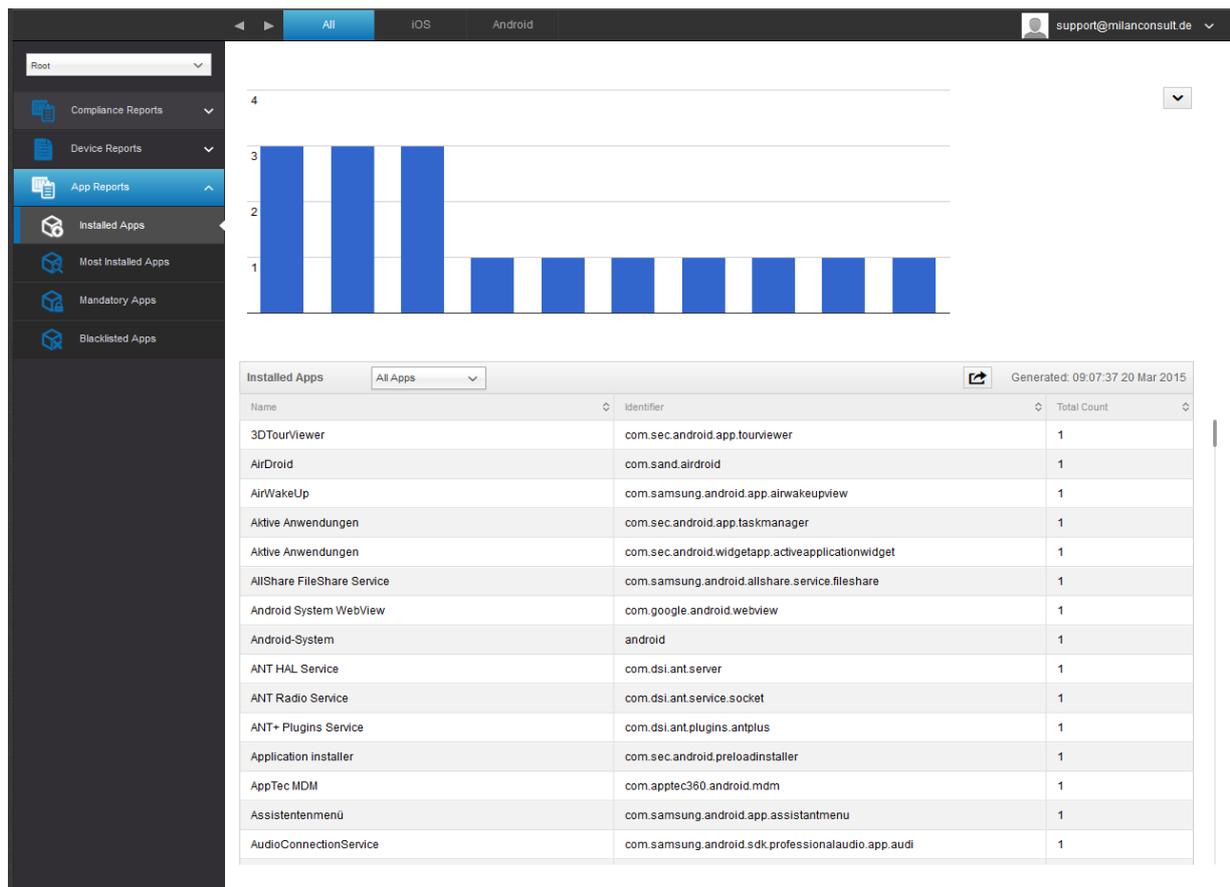
Installed Apps

Hier erhalten Sie eine Übersicht aller Apps die installiert worden sind.

Sie können dies anhand folgender Kriterien sortieren:

- All Apps (Es werden alle Apps berücksichtigt)
- System Apps (Es werden ausschließlich vom Gerätehersteller kommende Apps angezeigt)
- User Apps (Es werden ausschließlich die manuell installierten Apps angezeigt, offizieller AppStore und AppTec Enterprise Store)

Name	Name der jeweiligen App bzw. Dienst
Identifizier	Eindeutige ID der App / eines Dienstes
Total Count	Anzahl wie oft diese App / dieser Dienst auf den Endgeräten installiert ist



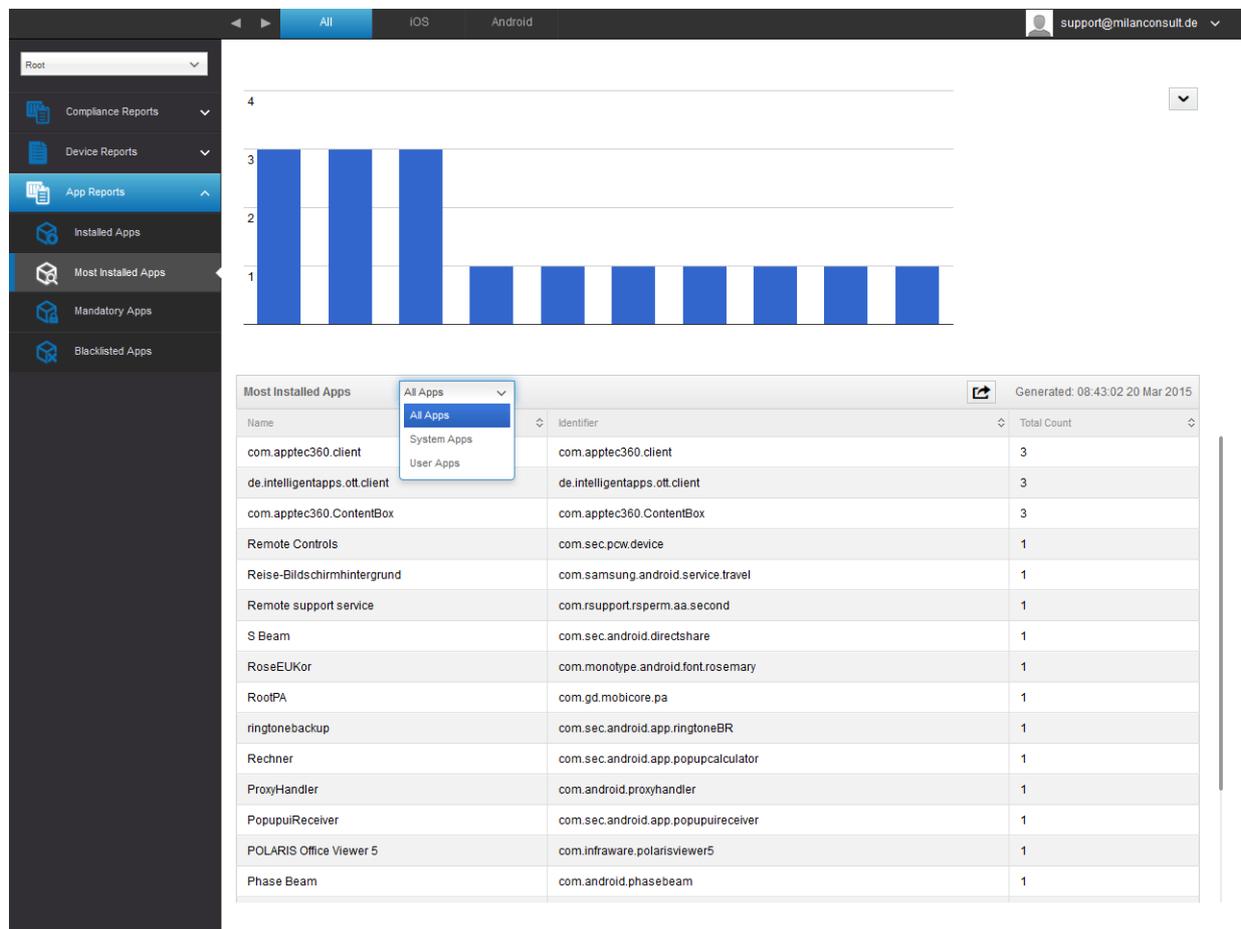
Most Installed Apps

Hier erhalten Sie eine Übersicht der meist installierten Apps.

Sie können dies anhand folgender Kriterien sortieren:

- All Apps (Es werden alle Apps berücksichtigt)
- System Apps (Es werden ausschließlich vom Gerätehersteller kommende Apps angezeigt)
- User Apps (Es werden ausschließlich die manuell installierten Apps angezeigt, offizieller AppStore und AppTec Enterprise Store)

Name	Name der jeweiligen App bzw. Dienst
Identifier	Eindeutige ID der App / eines Dienstes
Total Count	Anzahl wie oft diese App / dieser Dienst auf den Endgeräten installiert ist



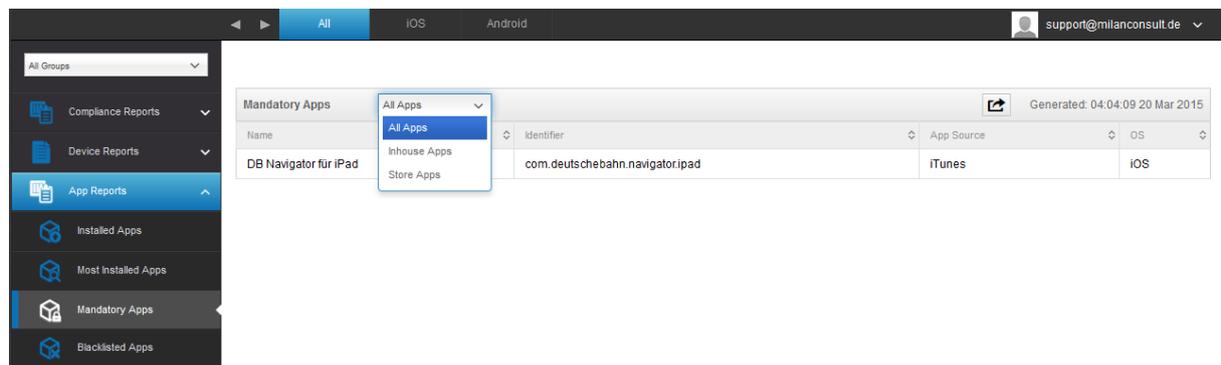
Mandatory Apps

Hier erhalten Sie eine Übersicht von allen Mandatory (zwingend erforderlichen) Apps.

Es kann zwischen folgenden Kriterien unterschieden werden:

- All Apps (Alle Apps)
- InHouse Apps (selbst hochgeladene / eigenentwickelte Apps)
- Store Apps (offizielle AppStore Apps)

Name	Name der jeweiligen App bzw. Dienst
Identifizier	Eindeutige ID der App / eines Dienstes
App Source	Für welchen AppStore es sich handelt: - Google PlayStore - iTunes AppStore (iOS) - Microsoft Store (Windows Phone=
Total Count	Anzahl wie oft diese App / dieser Dienst auf den Endgeräten installiert ist

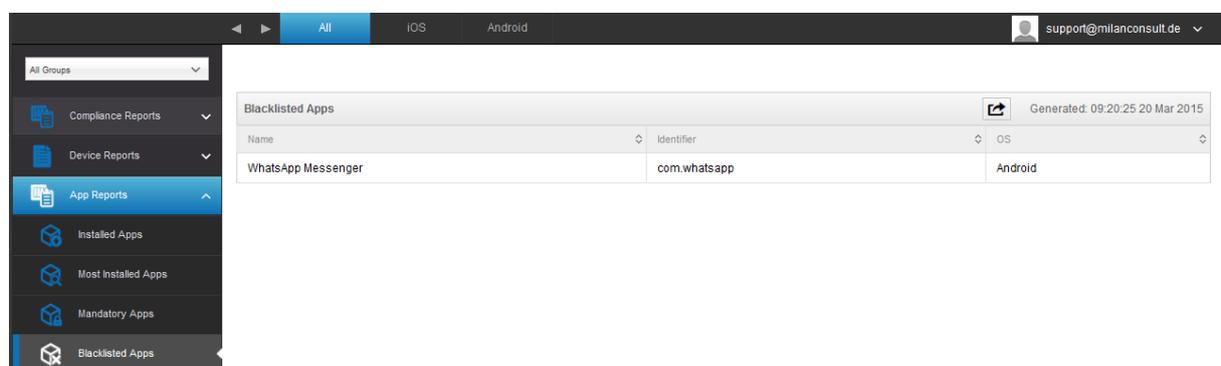


Name	Identifier	App Source	OS
DB Navigator für iPad	com.deutschebahn.navigator.ipad	iTunes	iOS

Blacklisted Apps

Hier erhalten Sie eine Übersicht über alle definierten Blacklisted Apps.

Name	Name der jeweiligen App bzw. Dienst
Identifizier	Eindeutige ID der App / eines Dienstes
OS	Um welche Plattform (Android, iOS, Windows Phone) es sich handelt



Name	Identifier	OS
WhatsApp Messenger	com.whatsapp	Android

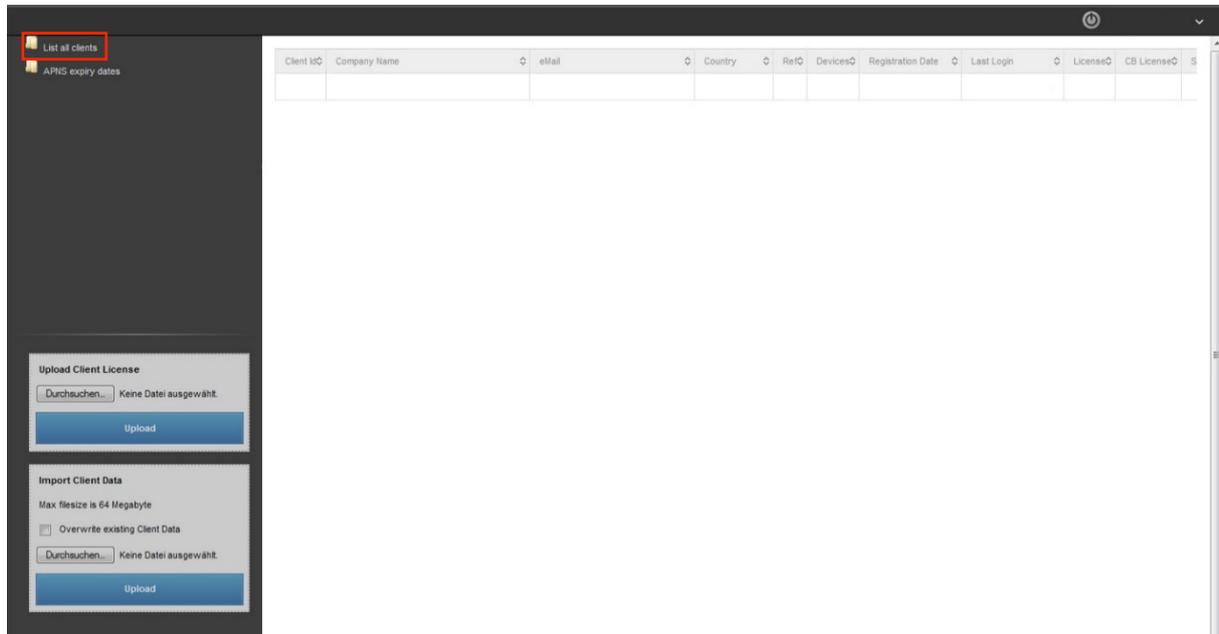
VI. Mandanten Management

Im Mandanten-Portal können weitere AppTec Lizenzen hochgeladen werden, welche daraufhin als neue AppTec-Instanz (genannt „Client“) fungieren. Im Endeffekt können also mehrere Clients mit einer Installation verwaltet und zur Verfügung gestellt werden.

Um die entsprechende Oberfläche zu öffnen, melden Sie sich bitte auf der Appliance mit den „Server Admin Credentials“ an, welche Sie während des Installationsvorgangs festgelegt haben („STEP THREE“ der Appliance Config).

Oberfläche

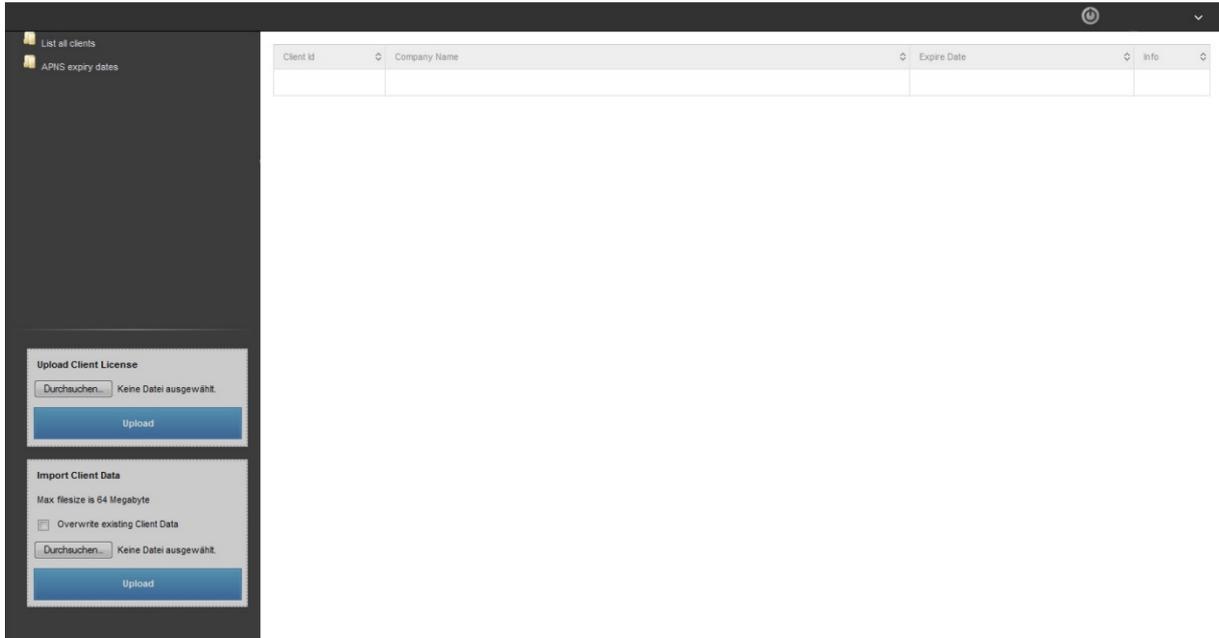
List all clients



Client ID	Client ID
Company Name	Firmenname
eMail	E-Mail Adresse der Kontaktperson
Country	Land
Ref	Ref
Devices	Anzahl an registrierten Geräten
Registration Date	Zeitpunkt der Lizenzinspielung
Last Login	Letzter Login des Admin Accounts
License	Anzeige des Lizenztyps (Free Paid)
CB License	Typ der ContentBox Lizenz (Free Paid)
Status	Aktueller Status des AppTec-Clients
Expired	Zeigt an, ob die Lizenz abgelaufen ist

Hier wird Ihnen eine Übersicht aller eingespielten AppTec-Clients angezeigt.

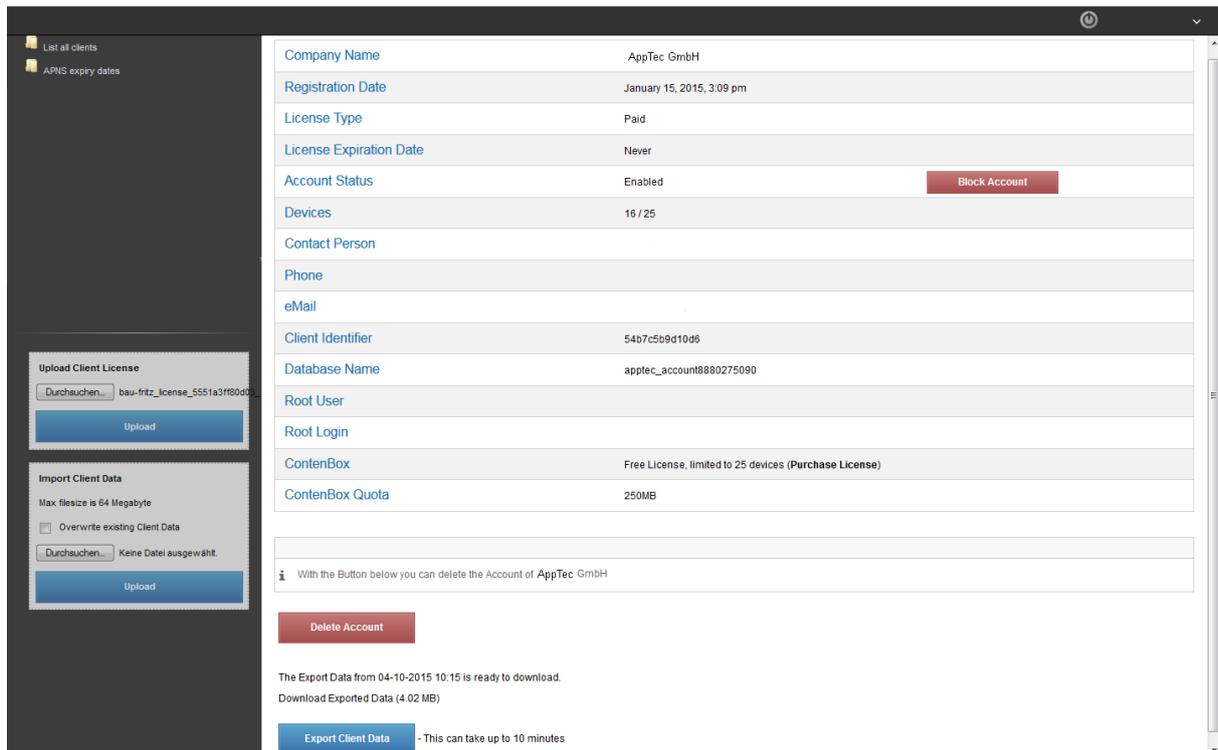
APNS expiry dates



Client ID	Client ID
Company Name	Firmenname
Expire Date	Ablaufdatum für das Apple APNS-Zertifikat
Info	Weitere Informationen

Auf dieser Übersichtsseite sind alle Ablaufzeitpunkte für die APNS Zertifikte notiert.

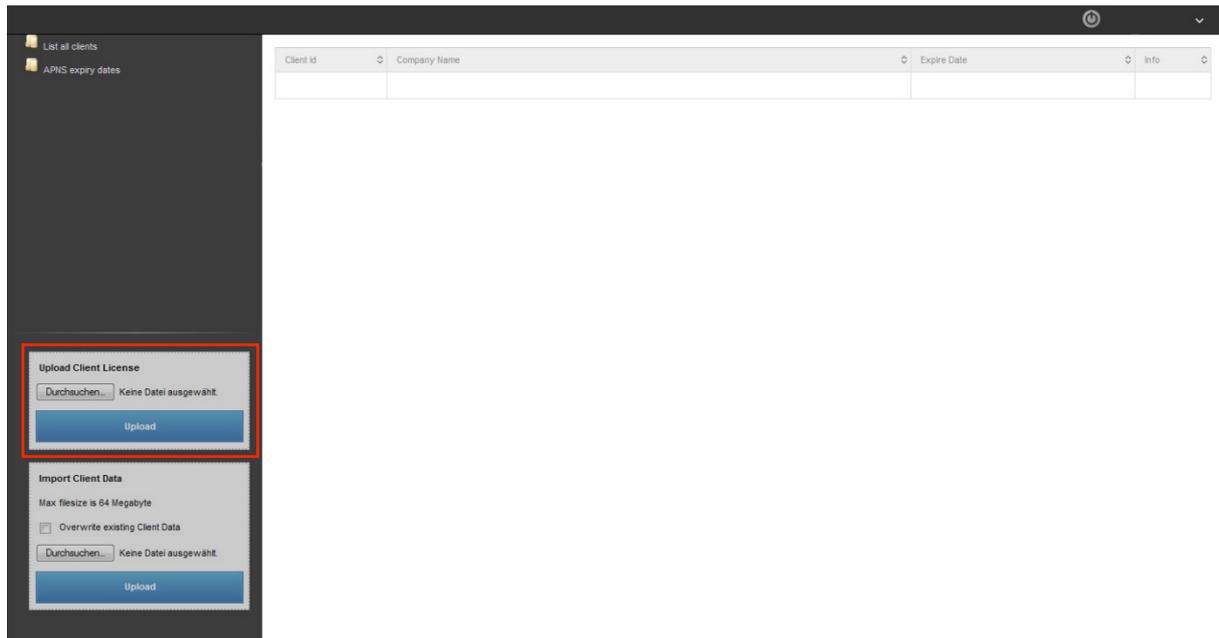
Account Information



Company Name	Firmenname
Registration Date	Zeitpunkt der Lizenzenspielung
License Type	Anzeige des Lizenztyps (Free Paid)
License Expiration Date	Ablaufdatum der Lizenz
Account Status	Status des Accounts (Enabled Disabled)
Devices	Anzahl an registrierten Geräte
Contact Person	Kontaktperson
Phone	Telefonnummer der Kontaktperson
eMail	Email Adresse der Kontaktperson
Client Identifier	Kennnummer des AppTec-Clients
Database name	Datenbankname der AppTec-Clients
Root User	Vollständiger Name des Root Users
Root Login	Loginname des Root Users (Email)
ContentBox	Lizenzinformationen bzgl. der Content Box
ContentBox Quota	Verfügbarer ContentBox-Speicherplatz

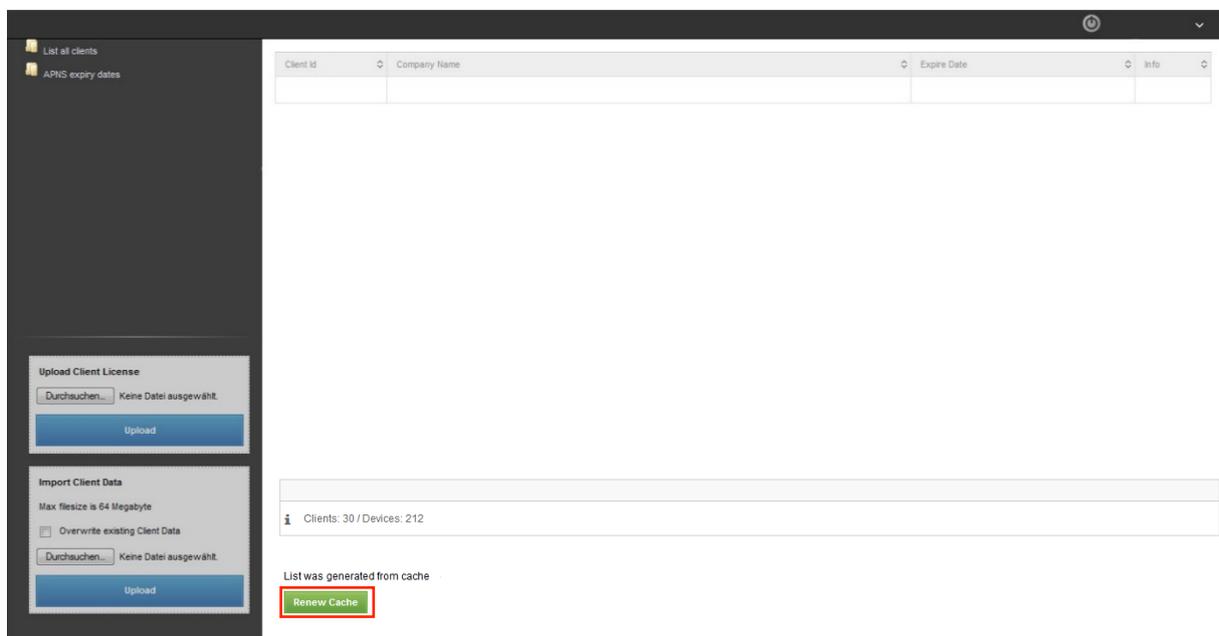
Block Account / Unblock Account	Nach einem Klick auf „Block Account“ ist kein Zugriff auf den AppTec-Client mehr möglich
Delete Account	Hier können Sie die AppTec-Client löschen
Export Client Data	Hier können Sie die Clientinformationen exportieren, um Sie z.B. auf einer neuen Instanz einzuspielen

Einspielen einer weiteren AppTec-Lizenz



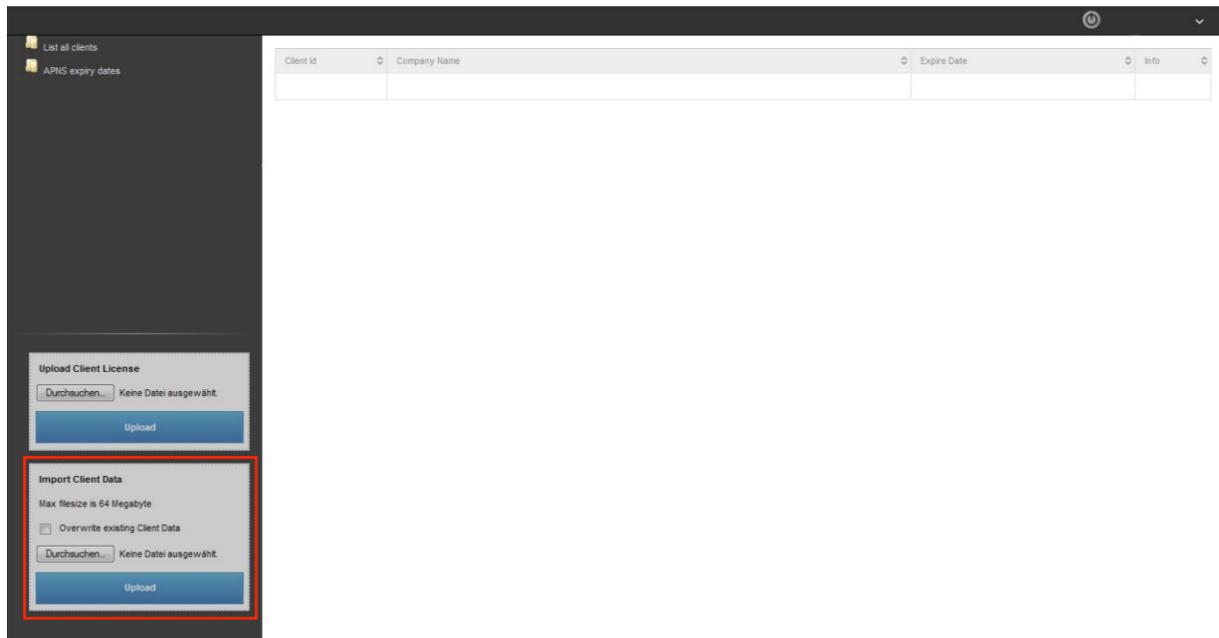
Nachdem Sie eine weitere AppTec-Lizenz erhalten haben, können Sie diese im Mandanten-Portal hochladen.

Klicken Sie hierzu auf „Durchsuchen“, wählen Sie die entsprechende Lizenzdatei aus und klicken danach auf „Upload“. Der neue AppTec-Client ist damit erfolgreich eingespielt.



Nach einem Klick auf „Renew Cache“, was ein Aktualisieren der Liste bewirkt, wird der neu eingespielte Client angezeigt.

Import eines Client-Backups



Wenn Sie ein Backup eines AppTec-Clients erstellt haben (über die „Export Client Data“ Funktion), dann können Sie dieses über den „Import Client Data“ Dialog wieder auf ein System einspielen.

Klicken Sie auf „Durchsuchen“, um die entsprechende Datei auszuwählen und hochzuladen. Danach ist das Backup auf der Appliance eingespielt.

Wenn Sie zuvor noch „Overwrite existing Client Data“ aktivieren, so wird beim Einspielen eines bereits bekannten Clients kein neuer Eintrag erstellt, sondern der jeweilige Eintrag aktualisiert/überschrieben.

KONTAKT

Noch fragen? Kontaktieren Sie uns einfach unter:

Für allgemeine technische Fragen

support@apptec360.com

+41 61 511 3210

Für Fragen bzgl. der Installation einer virtuellen Appliance

consulting@apptec360.com

+41 61 511 3214

DISCLAIMER

© AppTec GmbH

Diese Dokumentation ist urheberrechtlich geschützt. Alle Rechte liegen bei der AppTec GmbH. Jede andere Nutzung, insbesondere die Weitergabe an Dritte, Speicherung innerhalb eines Datensystems, Verbreitung, Bearbeitung, Vortrag, Aufführung und Vorführung sind untersagt. Dies gilt sowohl für das gesamte Dokument als auch Teile davon. Änderungen vorbehalten.

Andere, an dieser Stelle nicht ausdrücklich aufgeführte, Firmen-, Marken- und Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Inhaber und unterliegen dem Markenschutz. Änderungen und Irrtümer vorbehalten.